A propos de l'avis de la Commission de la protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires

Burton, Cedric; Poullet, Yves

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2005

Document Version
le PDF de l'éditeur

Commission de la protection de la vie privée, avis n° 09/2005 du 15 juin 2005

Note d'observations de Cédric BURTON et Yves POULLET

COMPÉTENCE DE RÉGULATION EN MATIÈRE DE VIE PRIVÉE – DONNÉES À CARACTÈRE PERSONNEL – DONNÉES JUDICIAIRES – LISTES BLANCHES – LISTES NOIRES – VIE PRIVÉE.

Dans son avis, la Commission de la protection de la vie privée réaffirme l'application de la législation de protection des données à caractère personnel aux listes noires. Elle y souligne quelques lacunes de l'actuelle législation et opte pour un encadrement du phénomène par une norme législative.

La Commission de la protection de la vie privée;

Vu la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en particulier l'article 29;

Vu la demande d'avis du 18 mars 2005 de la Ministre de l'Emploi, chargée de la Protection de la Consommation sur un encadrement des listes noires;

Vu le rapport de Madame M. Salmon et Monsieur P. Poma;

Emet, le 15 juin 2005, l'avis suivant:

I. Objet des demandes: listes noires dans le secteur privé

1.1. Par lettre du 18 mars 2005, la Ministre de l'Emploi, chargée de la Protection de la Consommation demande à la Commission, d'une part d'émettre un avis sur la nécessité d'encadrer les listes noires, d'autre part de préciser les principes utiles à cet encadrement et d'indiquer si les éléments mentionnés dans la demande sont adéquats, et enfin, de s'exprimer sur la méthode qui lui semble la plus convenable à cet égard pour une meilleure efficience des règles de protection de la vie privée.

1.2. Vu la formulation de la demande d'avis susmentionnée et la déclaration gouvernementale (voir ci-après), la Commission estime également approprié de ne s'exprimer, dans le cadre du présent avis, que sur les listes noires existantes et/ou les éventuelles listes noires non réglementées dans le secteur privé.

II. Un choix entre diverses options

2.1. La Commission a pris connaissance de la «Déclaration de politique fédérale du 12 octobre 2004», dans laquelle, sous l'intitulé «(5) Les nouveaux besoins sociaux et défis de société», le Gouvernement signale qu'il entend se pencher sur un certain nombre de nouveaux défis de société. On y lit encore: «Dans notre société d'information moderne, l'individu est en effet submergé par une telle quantité d'offres et d'informations qu'il n'est pas évident pour lui d'apprécier la fiabilité de certains informations (...). La technologie informatique moderne occupe une part toujours plus importante des flux d'information. Il importe d'éviter que l'on porte atteinte à la vie pri-

vée du citoyen par la création de tout type de banque de données.

Mais, d'autre part, il faut éviter qu'un écart social ne se creuse. C'est pourquoi le Gouvernement mettra en oeuvre un plan pour surmonter la fracture numérique. En outre, il faut accorder une attention à la sécurité des réseaux informatiques».

La Commission y voit l'expression d'une volonté d'encadrer les bases d'informations qui porteraient atteinte à la vie privée des citoyens.

2.2. Afin d'être complet, il faut également remarquer que la Commission a pris connaissance d'une proposition de loi du 31 mars 2005, introduite par Madame Annemie Roppe, membre de la Chambre des représentants.

Le but de cette proposition est d'interdire l'utilisation de listes noires en modifiant l'article 5 f) de la LVP.

2.3. Entre un éventuel encadrement normatif ou une interdiction totale, d'autres options sont possibles: une réglementation par des codes de conduites (article 44 LVP) et l'instauration de conditions particulières par arrêté royal pris après avis de la Commission (article 17bis LVP) et éventuellement, l'obligation d'obtenir une autorisation préalable.

2.4. Un choix s'impose entre ces options. La Commission souhaite défendre dans cet avis l'option de l'encadrement normatif, ceci sur la base des arguments qui seront développés ci-après (voir point 4.1.).

III. Historique des évaluations des listes noires par la Commission

Depuis 1998, la Commission a émis divers avis en matière de listes noires, particulièrement:

3.1. L'avis n° 8/98 du 25 février 1998 sur le projet de loi relatif aux jeux de hasard et aux établissements de jeux de hasard dans lequel la Commission invite le législateur à se saisir de l'occasion pour se prononcer sur la légalité et légitimité de liste noires que dresseraient et se communiqueraient des établissements de jeux, et qui reprendraient les coordonnées de joueurs indésirables, soit parce que ces personnes ont un comportement répréhensible (tricheurs, voleurs), soit parce qu'elles ne seraient pas rentables pour l'établissement. Sans remettre en cause la liberté de contracter des établissements de jeux constitués sous la forme de cercles privés, la Commission a estimé que les données traitées pour sélectionner des clients doivent rester proportionnées par rapport au but. S'il est compréhensible qu'un établissement veuille empêcher son accès à des tricheurs (notion à définir), ou à des personnes qui ont commis des infractions pénales dans l'établissement, il semble excessif d'enregistrer un client sur une liste noire commune à d'autres établissements du simple fait qu'il n'est pas rentable.

3.2. L'avis d'initiative n° 21/2000 du 28 juin 2000 relatif au fichier RSR, géré par le Groupement d'Intérêt Economique DATASSUR qui contient, outre de sérieuses critiques sur la légalité du fichier, une demande pressante de la Commission pour que les pratiques dénoncées soient interdites, ou fassent l'objet d'un encadrement légal, sans préjudice, dans l'intervalle, d'une suspension de ce fichier.

Il ressort du rapport annuel 2004 de Datassur que le nombre de «nouveaux» mauvais payeurs sur la liste noire des assureurs en 2004 a augmenté pour la première fois en trois ans . Fin 2004, les assureurs avaient ajouté 44.162 mauvais payeurs à la liste, ce qui représente 10 pour cent de plus qu'un an auparavant.

Selon Assuralia, le fichier Datassur compterait des mentions qui concerneraient des contrats d'assurance de dommage et reposeraient aussi bien sur le défaut de paiement (78%) que sur l'histori-

que des dommages (14%) et sur la fraude (3 %).

3.3. L'avis d'initiative n° 22/2000 du 28 juin 2000 relatif au traitement de données personnelles par certaines sociétés de renseignement commercial à partir des informations inscrites au rôle général des cours et tribunaux du travail dans lequel la Commission attire l'attention du Collège des Procureurs Généraux sur les pratiques de certaines sociétés qui utilisent le rôle général des tribunaux du travail pour enregistrer, dans leur base de données, les employeurs en litiges avec l'ONSS et ensuite, vendre ces informations à une clientèle constituée essentiellement d'organismes financiers. La Commission a estimé que ce type de traitement par les sociétés viole le principe de proportionnalité édicté à l'article 4 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (LVP) et l'article 8 de la même loi pour le traitement des données judiciaires. La Commission a également demandé au Collège des Procureurs Généraux de prendre les mesures adéquates à l'égard de cet usage incompatible des données du rôle.

3.4. L'avis n° 31/2000 du 9 novembre 2000 sur l'avant-projet de loi relatif à la Centrale des Crédits aux Particuliers, dans lequel la Commission n'a pas mis en question la légitimité de l'instauration d'un volet positif (enregistrement des contrats conclus) renforçant la lutte contre le surendettement et l'existence d'un volet négatif (contrats défaillants). Cependant, elle a salué l'instauration d'un Comité d'accompagnement et demandé à pouvoir y être représentée .

3.5. Confrontée à la constitution d'un fichier externe des locataires défaillants, la Commission a estimé, dans l'avis n° 52/2002 du 19 décembre 2002, que, d'une part l'instauration d'un tel fichier requiert une intervention préalable spécifique du législateur afin de l'autoriser éventuellement et le cas échéant, d'en spécifier les modalités de son choix et, d'autre part ce fichier n'était pas compatible avec les articles 4, 9, 17 et 18 de la loi du 8 décembre 1992.

IV. Examen de la demande

4.1 Nécessité d'un encadrement des listes noires du secteur privé

Tout d'abord, la Ministre de l'Emploi, chargée de la Protection de la Consommation demande à la Commission de confirmer, ou non, ses avis antérieurs sur la nécessité d'encadrer les listes noires.

En se référant aux avis mentionnés sous le titre III, la demande de réglementer les listes noires dans le secteur privé peut, selon la Commission, reposer sur divers fondements. La Commission attire l'attention sur les arguments suivants :

4.1.1. Définition de la «liste noire» et demande de critères uniformes harmonisés par le Groupe 29

Comme la Ministre de l'Emploi, chargée de la Protection de la Consommation et le Ministre des Affaires sociales et de la Santé publique, la Commission constate que le consommateur est confronté à un nombre croissant de bases de données à caractère personnel mises en oeuvre par le secteur privé et qui rentrent dans la définition donnée par le Groupe de protection des données institué en application de l'article 29 de la directive européenne 95/46/CE dit «Groupe 29», à savoir, «Les listes noires consistent à collecter et à diffuser certaines informations concernant un groupe donné de personnes, élaborées conformément à certains critères en fonction du type de liste noire dont il s'agit, se traduisant en règle générale par des effets nocifs et préjudiciables pour les personnes qui y figurent. Ces effets peuvent entraîner la discrimination d'un groupe de personnes en les privant de toute possibilité d'accès à un service déterminé ou en nuisant à leur réputation.»

La Commission souscrit à cette définition de la «liste noire» du Groupe 29. Elle précise que celle-ci ne vise que les traitements dont la finalité est de permettre la communication (accès, consultation,...) à des tiers et elle invite l'autorité normative à s'y référer dans le cadre de l'adoption d'une norme éventuelle.

La Commission rappelle que deux conclusions fondamentales ont été tirées par le «Groupe 29» à l'issue de ce travail:

– l'incidence et les effets néfastes de ces fichiers dans la sphère privée et sociale des individus;

– l'existence de divergences manifestes dans le contenu de la réglementation de ces fichiers et sa mise en oeuvre dans chaque Etat membre.

En conséquence, le Groupe 29 appelait à pouvoir disposer de critères uniformes et harmonisés pour les traitements de type «listes noires» de données à caractère personnel.

La Commission entend souligner que, si l'adoption de tels critères n'est pas encore une réalité au sein de l'Union européenne, elle estime néanmoins que l'incidence néfaste des listes noires dans le secteur privé mises en oeuvre sur base de critères non harmonisés et non uniformes requiert une intervention de la part des autorités de chaque pays membre, c'est-à-dire un encadrement des listes noires.

4.1.2. Multiplication des listes noires non réglementées par le secteur privé

Sans être exhaustive, la Commission indique, ci-après, les listes noires (ou projets de listes noires) les plus singulières dont il a été question ces dernières années, sans que la Commission n'ait eu l'occasion de les apprécier sous la forme d'un avis spécifique.

a) Dès 1998, la Commission s'est préoccupée du fichier PREVENTEL qui centralise les données de clients des opérateurs de téléphonie lorsque ces clients se trouvent en situation de défaut de paiement.

A diverses occasions, elle a émis plusieurs réserves sur les modalités concrètes de fonctionnement de ce fichier, notamment, à propos de la détermination précise de l'objectif poursuivi, des conditions de l'enregistrement des données, de l'information des personnes fichées et de leur droit d'accès. Lorsque le système a commencé à être appliqué, des dérives se sont manifestées par l'utilisation de la menace de fichage afin de faire pression sur les clients qui contestent le bien fondé d'une facture.

b) La Commission a été informée d'un projet du secteur pétrolier d'instaurer un fichier dit des «Door Raiders» qui enregistre par caméras les plaques minéralogiques des véhicules qui s'approvisionnent en carburant et partent sans payer.

c) Secteur de la grande distribution

Des éléments à disposition de la Commission donnent à penser que des fichiers, plus ou moins centralisés, de suspicions de fraude, de vol etc. ont été mis en place dans le secteur de la grande distribution.

Ainsi, il est question, depuis des décennies, de la gestion centrale de données à caractère personnel en matière de constats de vols commis par les clients. Les constats de vol par les supermarchés participants sont repris dans des formulaires uniformes de constat, envoyés à une ASBL (l'ASBL Prévention et sécurité), qui traite les données à caractère personnel pour établir des statistiques de délit au profit des membres de l'ASBL et effectuer la gestion globale des constats de vol au profit de ses membres, c'est-à-dire la communication des formulaires de constat à la police et au parquet. Fin 2004, selon un supermarché participant, 66.955 constats (il ne s'agit pas du nombre des personnes) auraient été enre-

gistrés depuis 2001 dans la base de données de l'ASBL Prévention et Sécurité, de sorte que le nombre actuel de personnes enregistrées se situe certainement dans les dizaines de milliers.

Enfin, à l'instar de la gestion existante des constats de vol, la presse de 2004 a évoqué des projets visant à instaurer une liste noire similaire, avec participation des commerçants indépendants affiliés à l'UNIZO .

d) Secteur de la distribution de l'énergie

En 2004, la Commission a été contactée par la «Beroepsvereniging der brandstoffenhandelaars van Oost-Vlaanderen» (Union professionnelle des fournisseurs de combustibles de Flandre orientale) à propos d'un projet de constitution d'un fichier des mauvais débiteurs pour les fournitures de mazout.

Une velléité comparable s'était déjà manifestée, il y a 7 à 8 ans, de la part d'une fédération de fournisseurs de matériaux de construction.

L'existence de cette demande et de récents articles de presse indiquent un réel risque d'émergence d'un grand nombre de listes noires non réglementées de mauvais payeurs dans le marché libéralisé de l'énergie (donc non seulement dans le domaine des combustibles mais également dans celui de la fourniture d'électricité et/ou de gaz, par exemple).

e) Le Syndicat National des Propriétaires (SNP)

En 2002, la Commission a estimé que l'instauration d'un fichier des locataires défaillants requérait une intervention préalable spécifique du législateur (cf. 3.5. ci-avant).

Par la suite, pour des raisons propres, semble-t-il, non liées à cet avis, le SNP a décidé de résilier le contrat conclu avec la société Checkpoint qui gérait la liste.

Cependant, tout récemment, la presse a rapporté l'intention manifestée par le SNP de mettre en service un nouveau fichier des locataires défaillants pour le second semestre de l'année 2005, le SNP considérant, en dépit de l'avis de la Commission, que cela n'est pas illégal.

4.1.3. Limitations dans le cadre normatif actuel

Quelques principes de base de la LVP démontrent que l'actuel cadre normatif (la LVP) n'est pas suffisant pour mettre en oeuvre légalement plusieurs listes noires. En principe, l'intervention d'une loi formelle, voir point 4.3. , est requise pour pouvoir établir des listes noires dans le secteur privé. Cette loi, soit déroge aux principes de la LVP énoncés aux articles 5, 7, 8 et 9 de la LVP, soit les complète.

a) Article 5 f) de la LVP Equilibre des intérêts en présence

Les divers responsables dans le secteur privé invoquent fréquemment qu'ils ont un intérêt économique important à établir des listes noires (lutter contre la fraude commise par des clients). Cependant, un tel intérêt doit être examiné, au cas par cas, au regard de l'article 5 f) de la LVP et, in concreto, de l'article 4 de la LVP; la base juridique d'un tel traitement est donc inexistante ou du moins douteuse.

b) Article 7 de la LVP Données médicales

Dans quelques secteurs, il est devenu courant d'enregistrer les données personnelles médicales du client (par exemple, dans le secteur des assurances).

La Commission rappelle que le traitement de ces données à caractère personnel doit être conforme à l'article 7 de la LVP.

Bien que l'assureur individuel puisse, peut-être, alléguer que des informations sur les risques médicaux sont nécessaires afin d'évaluer les risques liés à un client précis lors de la conclusion de la police (calcul de la prime, ...), la Commission estime que les données personnelles médicales n'ont pas leur place dans des listes noires, c.-à-d. en dehors de la gestion des risques client par l'acteur individuel dans le secteur privé.

c) Article 8 de la LVP

Nombre de données à caractère personnel traitées dans les bases de données de type «listes noires» portent sur des éléments liés à l'un ou l'autre des concepts visés à l'article 8 de la LVP (litige, suspicion, poursuite, condamnation ayant trait à des infractions). Le principe (voire la portée) de l'interdiction de traiter de telles données et les exceptions doivent être clairement définis.

A propos de certains enregistrements qui incluent des risques alourdis pouvant conduire à une procédure , la Commission a considéré dans l'avis «Datassur» que «Bien que ces données ne soient pas des données judiciaires au sens de l'article 8 de la loi, le traitement de telles données a un caractère plus dommageable et plus délicat encore, dans la mesure où elles n'ont pas été soumises à l'examen du juge ni à une quelconque procédure contradictoire. Traiter des données aussi peu fiables entre également en porte-à-faux avec le principe d'exactitude inscrit à l'article 4, § 1er, 4° de la loi.

Il résulte de ce qui précède qu'un groupement sectoriel représentatif des entreprises d'assurance ne peut traiter, sans qu'une législation particulière ne l'y autorise, ni des données visées à l'article 8 de la loi, ni des données déduites de faits objectifs sans faire mention de ces faits.»

d) Article 9 de la LVP Droit à l'information

Dans le secteur privé, il est parfois soutenu qu'une exception au devoir d'information, lors de l'enregistrement dans la liste noire, serait justifiée, en raison d'intérêts privés de recherche ou d'obligations du responsable, de l'importance de la protection des sources ou encore, du risque qu'une communication de l'enregistrement dans une liste noire produise un effet non désiré (utilisation d'une fausse identité par l'intéressé, ...).

La Commission fait remarquer qu'actuellement, la LVP n'autorise pas d'exception appropriée aux intérêts des acteurs dans le secteur privé, même si ceux-ci souhaitent une exception au devoir d'information en matière de listes noires.

Certes, l'article 3, § 5, 4° de la LVP énonce, notamment, que l'article 9 ne s'applique pas aux traitements de données rendus nécessaires par la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, mais il est strictement limité. Ainsi, les établissements de crédit et les entreprises d'investissement ont des devoirs spécifiques de diligence afin de prévenir l'utilisation du système financier pour le blanchiment d'argent et le financement du terrorisme sur la base de la loi précitée et des règlements et circulaires de la Commission bancaire, financière et des assurances («CBFA») sur la base de cette loi .

L'article 13.1 de la Directive européenne 95/46/CE permet à l'autorité d'introduire une exception au devoir d'information moyennant une modification formelle de la LVP, si le législateur estime nécessaire l'instauration d'une liste noire dans le secteur privé afin de garantir la prévention, la recherche, la détection et la poursuite de faits punissables. Toutefois, la Commission fait observer qu'elle n'est pas en faveur de l'introduction d'exceptions

éventuelles au devoir d'information dans le secteur privé (cfr également 4.2.4., 4.2.6. et 4.3.1.b), car la dispense du devoir d'information pour la prévention, la recherche, la détection et la poursuite de faits punissables est réservée, à l'article 3, §,§ 4 et 5, aux autorités publiques expressément mentionnées dans cet article (par exemple, les services de police). En raison du lien étroit entre la prestation du service et la liste noire utilisée, la transparence du traitement des données à caractère personnel dans le secteur privé est cruciale pour le citoyen, parce que toute dérogation à la transparence entrave gravement les possibilités de contrôle (aucun contrôle n'est possible sur ce qu'on ignore).

Enfin, l'exception au devoir d'information pour les listes noires dans le secteur privé peut également avoir de sérieuses conséquences socio-juridiques (exclusion sociale sans que la personne concernée ne dispose des informations nécessaires pour combattre l'exclusion, aucun droit de défense, etc.).

4.1.4. Sécurité en droit

a) Pour les personnes concernées

Le préjudice et/ou l'exclusion liés à l'enregistrement dans une liste noire justifie des garanties complémentaires à celles données par la LVP.

b) Pour les responsables du traitement (risque légal)

Il ressort des contacts de la Commission avec différents responsables de traitement de type «listes noires» ou de candidats à la mise en oeuvre d'un tel traitement qu'un encadrement leur permettrait de définir des règles du jeu plus claires. En effet, la mise en place d'une banque de données impose des investissements financiers et humains importants de même qu'une prise en compte du risque légal.

4.1.5 Loi du 25 février 2003 tendant à lutter contre la discrimination et modifiant la loi du 15 février 1993 créant un centre pour l'égalité des chances et la lutte contre le racisme

Cette législation interdit toute discrimination directe ou indirecte, qui ne répond pas à une justification objective et raisonnable, fondée sur le sexe, une prétendue race, la couleur, l'ascendance, l'origine nationale ou ethnique, l'orientation sexuelle, l'état civil, la naissance, la fortune, l'âge, la conviction religieuse ou philosophique, l'état de santé actuel ou futur, un handicap ou une caractéristique physique lorsqu'elle porte, notamment, sur la fourniture ou la mise à la disposition du public de biens et de services, sur la diffusion d'un texte, d'un avis d'un signe ou de tout support comportant une discrimination, sur les conditions d'accès au travail, sur l'accès, la participation et tout autre exercice d'une activité économique, sociale, culturelle ou politique accessible au public.

On peut se demander si bon nombre de listes noires ne contiennent pas une ou plusieurs discriminations rejetées par la loi du 15 février 1993. Un encadrement normatif avec reconnaissance de la légitimité d'un nombre limité de finalités et de critères d'enregistrement pour les listes noires aidera, peut-être, l'autorité compétente à contrôler le respect de la loi du 15 février 1993 par les listes noires.

4.1.6. Droit comparé

Une brève étude comparative montre que nos voisins ont décidé, soit l'exigence d'une base normative pour les listes noires (par exemple, la France), soit des garanties auxquelles doivent répondre les listes noires dans le secteur privé, que ce soit ou non, avec l'exigence d'une analyse préalable de la liste noire par l'autorité de surveillance (par exemple, les Pays-Bas).

a) France

Position de la Commission nationale de l'informatique et des libertés («CNIL»)

La Commission nationale de l'informatique et des libertés relate dans son rapport que le législateur est intervenu pour encadrer des fichiers mutualisés pour en confier la gestion à une personne de droit public, avec des contraintes de services publics. Cela n'a pas abouti pour autant à la formulation d'un principe d'exclusivité. Le secteur privé (par exemple, assurances et télécommunications) a mis en oeuvre ses propres fichiers. La CNIL estime néanmoins qu'au nom du respect du principe de proportionnalité, il faut éviter que des fichiers à vocation sectorielle ne se muent en fichiers à vocation universelle.

Position du Conseil constitutionnel

La position du Conseil constitutionnel sur le projet de texte de loi adopté par le Sénat français le 15 juillet 2004, qui transposait en droit français la directive européenne du 24 octobre 1995, retient l'attention en ce qu'elle vise les listes noires de fraudeurs.

L'article 9 du texte disposait que les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûretés pouvaient être mis en oeuvre par les personnes morales victimes d'infractions ou agissant pour le compte des dites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi, dans les conditions prévues par la loi.

Le 29 juillet 2004, déférée devant le Conseil constitutionnel, cette disposition de la loi a été annulée au motif «qu'en raison de l'ampleur que pourraient revêtir les traitements de données personnelles ainsi mis en oeuvre et de la nature des informations traitées, (ndlr, le texte dont question) pourrait affecter, par ses conséquences, le droit au respect des libertés publiques; que la disposition critiquée doit dès lors comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution; considérant que, s'agissant de l'objet et des conditions du mandat en cause, la disposition critiquée n'apporte pas ces précisions; qu'elle est ambiguë quant aux infractions auxquelles s'applique le terme de 'fraude'; qu'elle laisse indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore, si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction; qu'elle ne dit rien sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations;

qu'au regard de l'article 34 de la Constitution, toutes ces précisions ne sauraient être apportées par les seules autorisations délivrées par la Commission nationale de l'informatique et des libertés; qu'en l'espèce et eu égard à la matière concernée, le législateur ne pouvait pas non plus se contenter, ainsi que le prévoit la disposition critiquée éclairée par les débats parlementaires, de poser une règle de principe et d'en renvoyer intégralement les modalités d'application à des lois futures; que, par suite, le 3° du nouvel article 9 de la loi du 6 janvier 1978 est entaché d'incompétence négative».

Dès lors, la CNIL a considéré que ces traitements destinés à lutter contre la fraude requièrent une disposition législative ad hoc, avec les garanties appropriées et spécifiques répondant aux exigences de la Constitution.

Si le renforcement de la lutte contre la fraude aux moyens de paiement rend légitime le souhait des professionnels de s'organiser au mieux pour faire face à cet impératif, seule une intervention législative spécifique paraît de nature à concilier les obligations des professionnels et les droits des personnes concernées, en imposant des règles communes, notamment, sur les garanties et conditions minimales d'inscrip-

tion dans de tels fichiers mutualisés à l'ensemble d'une profession.

b) Pays-Bas

Aux Pays-Bas, le 'College Bescherming persoonsgegevens' («CBP») (Collège de protection des données à caractère personnel) a constitué un dossier général de thèmes sur les listes noires publié sur son site web et qui se base sur un rapport antérieur de la CBP de mai 1995 .

L'approche énonce le principe que la «Wet bescherming persoonsgegevens», (Loi de protection des données à caractère personnel), ne nécessite pas un encadrement normatif complémentaire des listes noires, mais qu'une telle liste est interdite sans de bonnes garanties. Ces garanties se retrouvent sous la forme de l'exigence d'une analyse préalable par le CBP et l'utilisation d'une checklist:

Si des données pénales ou des données relatives à un comportement illégitime ou gênant figurent sur une liste noire avec l'intention d'échanger ces informations avec d'autres (un traitement de données au profit de tiers), le CBP doit, dans certaines situations, organiser une analyse préalable;

Sur la base des normes de la Loi de protection des données à caractère personnel, le Collège a également mis à disposition une checklist «Zwarte lijsten» pour le secteur privé. Il s'agit d'un réel fil conducteur pour organiser une liste noire aussi consciencieusement que possible. La checklist propose des questions de contrôle concrètes auxquelles il faut répondre pour pouvoir satisfaire aux normes de la Loi de protection des données à caractère personnel. Cette checklist est disponible sur le site web du Collège .

c) Conclusion

L'expérience à l'étranger démontre que, pour chaque liste noire dans le secteur privé, des garanties spécifiques et appropriées doivent être prévues efficacement. Toutefois les approches diffèrent sur la manière de procéder, c.-à-d. le point de vue selon lequel une réglementation complémentaire de ces garanties est requise ou non, l'exigence d'une analyse complémentaire préalable pour certaines listes noires, etc...

4.1.7. Divers arguments «pour et contre» les listes noires

Les partisans des listes noires en défendent l'utilisation avec les arguments suivants:

– avoir des intérêts légitimes de se protéger contre les clients à risque (nécessité économique des listes noires pour l'entreprise, liberté d'entreprise, liberté d'information, droit de propriété, ...);

– le fichage est purement indicatif, c.-à-d. qu'il laisse toute liberté aux fournisseurs de services de conclure ou non avec la personne fichée;

– les données sont contrôlées quant à leur exactitude, leur origine, etc.;

– la sécurité est totale: absence d'accès par des tiers non autorisés, respect des finalités;

– les droits des personnes sont respectés au-delà même des exigences de la LVP;

– les erreurs et/ou plaintes sont rares.

Les adversaires des listes noires invoquent souvent les aspects négatifs suivants:

– l'existence d'un risque d'exclusion sociale; généralement, une personne fichée n'obtient pas le service ou l'obtient à des conditions moins avantageuses;

– la masse de données enregistrées dans certaines banques empêche un contrôle réel et efficace de la qualité des données;

– des violations de confidentialité et l'absence d'identification de leur auteurs sont rendues possibles par une sécurité insuffisante et/ou un manque de formation des participants, particulièrement dans le chef des interlocuteurs directs («au guichet») avec la personne fichée;

– le fichage est détourné de sa finalité originelle. Une liste noire créée pour une finalité déterminée (par exemple, la lutte contre le surendettement) est également utilisée comme moyen de contrôle à l'égard des candidats à un emploi;

– es erreurs humaines fréquentes dues à la complexité du système en place, l'inadéquation du système.

Une approche normative des listes noires dans le secteur privé avec un encadrement efficace des risques possibles qu'elles engendrent semble une réponse adéquate aux arguments des tenants et opposants des listes noires.

4.1.8. Conclusion

Sur la base de ses avis antérieurs et des arguments qui précèdent, la Commission estime que pour les listes noires dans le secteur privé, des garanties spécifiques et appropriées doivent être prévues au moyen d'une solution normative. Selon elle, cette option normative devrait être préférée aux solutions alternatives indiquées ci-dessus au point 2.3.

4.2 Principes de références à appliquer aux listes noires

La Ministre de l'Emploi, chargée de la Protection de la Consommation demande à la Commission de préciser les principes utiles à l'encadrement des listes noires.

La Commission considère que, sauf une modification expresse à la LVP, une précision des principes utiles à l'encadrement des listes noires ne pourrait, en aucun cas, porter préjudice à l'application de la LVP.

Cela signifie que la norme spécifique recommandée par la Commission devrait encadrer les listes noires plus rigoureusement que la LVP. La Commission formule ci-après quelques propositions concrètes à destination de l'autorité normative («proposition normative additionnelle») après l'exposé de chaque principe.

Les principes suivants devraient être pris en considération:

4.2.1. Exigence d'une évaluation de la légitimité de la liste noire (article 5 de la LVP)

Sur la base de l'article 5 de la LVP, tout traitement de données à caractère personnel, sous la forme d'une liste noire, n'est, en principe, pas autorisé, à moins que ce traitement ne puisse s'appuyer sur l'un des motifs d'admissibilité mentionnés dans le même article.

Les acteurs privés se réfèrent actuellement, soit à l'article 5, a) de la LVP (consentement de la personne concernée), soit à l'article 5, f) de la LVP (l'intérêt de l'acteur privé est légitime et prévaut) pour légitimer la liste noire.

Toutefois, à défaut d'un encadrement normatif, aucune des deux pistes n'offre une garantie convaincante.

En effet, comme il ressort des considérations et avis susmentionnés (voir 3.1. et suivants), la Commission estime nécessaire un encadrement normatif des listes noires dans le secteur privé, parce que les listes noires non réglementées dans ce secteur bénéficient d'une légitimité insuffisante au regard de l'article 5, a) et/ou 5, f) de la LVP. Les motifs repris à l'article 5, a) et 5, f) de la LVP reposent également, de facto, sur une interprétation unilatérale du secteur, imposée sans négociation ou contradiction préalable.

Ainsi, l'exigence de la liberté du consentement (article 1, § 8 de la LVP) semble pro-

blématique si ce consentement constitue la condition pour obtenir un service essentiel à la personne concernée (par exemple, le consentement à l'utilisation des données médicales lors de la conclusion d'une assurance solde restant dû comme condition pour contracter un prêt hypothécaire ou lors de la souscription d'une assurance obligatoire RC pour les véhicules motorisés, ...).

4.2.2. Exigence d'une autorisation préalable de la Commission

Sauf dans les cas où une législation spécifique émet des exigences particulières à l'égard de la personne responsable du traitement pour la mise en oeuvre d'un traitement et, sauf l'application de l'article 41, § 2 de la LVP, toute personne peut mettre en oeuvre un traitement de liste noire après l'avoir déclaré auprès de la Commission.

Proposition normative additionnelle:

Aux yeux de la Commission, la complexité de la mise en oeuvre d'une banque de données centralisée, et donc l'appréciation des compétences requises, justifie que les responsables de listes noires, qui contiennent des données dont le traitement porterait atteinte à un droit fondamental prévu par la Constitution ou à des services considérés comme essentiels par une autorité normative, soient soumis à une autorisation préalable de la Commission.

A défaut d'une autorisation préalable, la liste noire ne pourrait être mise en oeuvre.

Sans qu'il ne lui appartienne de se prononcer de façon définitive sur la compatibilité de la procédure d'autorisation suggérée avec le droit européen, la Commission relève que l'article 20 de la Directive européenne 95/46 relative à la protection de la vie privée dispose comme suit:

«1. Les Etats membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en oeuvre.

2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle.

3. Les Etats membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées.»

4.2.3. Principe de finalité (article 4, § 1er, 2°, 3° et 4° de la LVP)

a. Obligation de décrire les finalités

Selon l'article 4, § 1, 2° de la LVP, pour chaque liste noire, la (les) finalité(s) doive(nt) être explicite(s).

On peut déduire du même article que tout encadrement normatif d'une liste noire doit énumérer, très clairement et de manière limitative, les diverses finalités pour lesquelles l'utilisation d'une liste noire dans le secteur privé peut être considérée comme légitime.

Pour la sécurité juridique de la personne concernée et l'exigence de proportionnalité reprise à l'article 4, § 1, 3°) de la LVP, il est essentiel que la description de la (des) finalité(s) soit aussi précise que possible, et donc pas générale comme «la lutte contre les risques client». Des descriptions plus spécifiques sont recommandées, par exemple, «la lutte contre le défaut de paiement».

b. Critères d'enregistrement

Une fois la (les) finalités de la liste noire décrite(s), la réglementation doit clarifier sur la base de quels critères le responsable

peut atteindre cette (ces) finalité(s). En effet, c'est au regard de ces critères que la personne concernée pourra être enregistrée, ou non, dans la liste noire.

En vertu de l'article 4, § 1, 3° et 4° de la LVP, il importe que:

la description de chaque critère d'enregistrement soit claire et précise. En effet, il faut distinguer entre les risques «client» qui sont pertinents, ou non, dans une liste noire, sans énoncer de manière générale les risques qui veulent être évités. Le citoyen peut se trouver dans de nombreuses situations diverses; ainsi il peut avoir déjà avoir été victime ou coupable dans une ou plusieurs circonstances dommageables, que ce soit en engageant sa responsabilité directe ou non, être responsable de factures restées impayées avec ou sans condamnation, avec ou sans protestation, recours en appel. En outre les critères généraux d'enregistrement peuvent contenir des aspects illégaux et/ou socialement inacceptables (par exemple, le fait d'habiter une certaine région, la race ou l'ethnicité de la personne concernée, ...);

chaque critère d'enregistrement soit proportionnel en fonction de la finalité visée et de son impact sur les intérêts de la personne concernée; cela signifie que le critère d'enregistrement doit être considéré comme suffisamment sérieux pour atteindre l'objectif. Par exemple, il serait disproportionné d'enregistrer une personne sur la base d'un montant impayé de 25 EUR;

les critères d'enregistrement soient énumérés de manière limitative (l'enregistrement dans la liste noire constitue en effet l'exception, et non la règle);

Les critères d'enregistrement soient objectifs; un montant minimum impayé et facturé en principal est objectif. La mention «peu fiable» ne l'est pas. Ceci est particulièrement important en termes d'exactitude et au point de vue de la contestation par la personne concernée;

En cas de doute sur la conformité des faits au regard d'un critère d'enregistrement (par exemple, y a-t-il eu protestation ou non), le client doit bénéficier du doute et de la présomption d'innocence, la charge de la preuve incombant au créancier.

4.2.4. Principe de proportionnalité (article 4, § 1er, 3° de la LVP)

a. Condition de l'enregistrement dans des listes noires

Les adversaires des listes noires dans le secteur privé soutiennent parfois que l'enregistrement dans une telle liste constitue une sanction privée imposée à l'intéressé par une instance qui est juge et partie, sans droit de défense pour l'intéressé.

En effet, l'enregistrement dans une liste noire constitue une sanction privée complémentaire qu'un fournisseur de services peut appliquer, sans qu'a priori, des garanties ne soient offertes et qu'une procédure contradictoire ne précède l'enregistrement sur la liste noire. Si les conditions d'enregistrement sur une liste noire peuvent être définies, fixées et/ou interprétées unilatéralement par un participant privé, le risque existe qu'il soit juge et partie, et également, qu'il puisse contraindre son client à effectuer un paiement que ce client estimerait indu ou contestable en le menaçant de l'inscrire sur une liste noire.

La Commission attire l'attention sur le fait que le principe du contradictoire constitue un des principes fondamentaux dans la conduite loyale d'un litige.

Certes, l'article 15 de la LVP prévoit actuellement un droit de contestation:

«Dès la réception de la demande tendant à faire rectifier, supprimer ou interdire d'utiliser ou de divulguer des données à caractère personnel ou dès la notification de l'introduction de l'instance visée à l'article 14, et jusqu'à ce qu'une décision soit coulée en force de chose jugée, le (respon-

sable du traitement) doit indiquer clairement, lors de toute communication d'une donnée à caractère personnel, que celle-ci est contestée».

Proposition normative additionnelle:

La Commission estime qu'au nom du droit à une procédure équitable et du principe de proportionnalité, un encadrement normatif des listes noires dans le secteur privé doit accorder une attention renforcée à ce droit de contestation, en particulier, en adoptant les dispositions suivantes:

Contestation auprès de la personne à l'origine de la communication des données:

– la personne compétente pour enregistrer une autre sur la liste noire et recevoir la contestation doit être déterminée avec précision et connue de la personne enregistrée (voir 4.2.7. a);

– la notification d'une contestation motivée par la personne enregistrée doit être mentionnée dans le fichier, selon la LVP; la norme devrait ajouter que si elle n'a pas pour effet automatique de radier immédiatement la personne, elle suspend la communication de ses données aux tiers; de plus, l'intéressé doit être clairement averti des effets de la contestation.

Détermination des recours:

Si la contestation n'aboutit pas à la rectification des données dans le sens souhaité, des recours non judiciaires doivent toujours être ouverts. Les modalités peuvent prévoir:

– un recours auprès d'un médiateur compétent pour le secteur auquel se rattache la liste; seule, l'introduction de ce recours à bref délai aurait pour effet de prolonger l'absence de communication des données aux tiers;

– un second recours, ayant le même effet suspensif, doit être ouvert auprès d'une autorité publique (par exemple, auprès du SPF Economie, Administration du Contrôle et de la Médiation) qui disposerait du droit d'ordonner la rectification des données et d'appliquer des sanctions administratives en cas de fichage injustifié.

– en toute hypothèse, la Commission pourrait être sollicitée par la personne ou par ces instances pour formuler un avis uniquement en matière de protection de la vie privé.

Liste noire traitant des données judiciaires:

Si une norme en matière de listes noires devait permettre le traitement de données judiciaires, il faut garder à l'esprit le principe de l'article 8 de la LVP et ne l'autoriser que dans des hypothèses spécifiques, après une mise en balance des intérêts concernés.

b. Délai de conservation dans la liste noire

L'article 4, § 1er, 5° de la LVP dispose que les données doivent être conservées sous une forme qui permet l'identification des personnes pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou traitées ultérieurement.

La Commission rappelle que le principe de proportionnalité implique que, lorsqu'une donnée n'est plus nécessaire par rapport à la finalité du traitement, elle doit être supprimée. Le droit à l'oubli doit l'emporter lorsqu'il est mis en balance avec le maintien de données dont la pertinence est douteuse. En effet, l'article 2 de la LVP dispose que, lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée.

Si, néanmoins, une durée de conservation s'impose en vertu d'une finalité encadrée, la fixation d'un délai de conservation

maximum des données est, en toute hypothèse , requise (3, 5 ou10 ans), qu'il y ait ou non une autorisation préalable de la Commission. La Commission rappelle qu'en tout état de cause, la durée de conservation doit être justifiée au regard du principe de proportionnalité.

c. L'existence d'alternatives pour les responsables

Il convient de se demander si le responsable, plutôt que de placer les clients sur une liste noire, n'aurait pas pu prendre d'autres mesures pour combattre les risques et si ces mesures alternatives n'auraient pas atteint efficacement la finalité visée. Les mesures alternatives doivent être préalablement répertoriées et évaluées. Si, par exemple, des supermarchés désirent mettre en oeuvre une liste noire des voleurs de magasins dans leur secteur, ils doivent, d'abord, adopter des mesures de prévention autres que la liste noire.

d. Nature du service interdit et existence d'alternatives pour les personnes concernées (article 4, § 1er, 3° de la LVP)

Le principe de proportionnalité implique l'examen de la mesure dans laquelle la personne concernée est exclue de certains services et s'il lui reste encore des alternatives.

En d'autres termes:

Chaque service est-il exclu ou l'exclusion est-elle limitée à un certain niveau de service ? Si par exemple, le citoyen ne paie pas sa facture pour le service de téléphonie mobile (GSM), risque-t-il d'être exclu de l'accès au service de téléphonie fixe, ou au contraire, seul le service impayé est-il suspendu ?

Quelle est la «portée» de la liste noire; celle-ci est-elle réalisée pour une seule entreprise (la Commission vise ici les situations de mono/oligopole), un groupe d'entreprises, un trust, un holding, un secteur, un pays ? Plus l'application territoriale de la liste noire est vaste, plus rapidement la liste devra être jugée disproportionnelle, sans garanties adaptées.

S'il reste au citoyen des alternatives auprès d'un concurrent et/ou d'une organisation qui fournirait un service social minimum analogue, les services universels seraient-ils compromis ? S'agit-il d'un service sous monopole, ... ?

e. Diffusion interne des données à caractère personnel parmi les employés des participants

Tant en raison des obligations de sécurité (voir ci-après) qu'en vertu du principe de proportionnalité, il semble recommandé que différents niveaux de protection soient instaurés en matière d'accès aux données à caractère personnel pour les collaborateurs des participants sur une base «need to know» (voir 4.2.11.).

Ainsi, un accès complet devrait être réservé à l'administrateur (technique) et/ou au préposé au traitement des données à caractère personnel alors qu'un accès complet n'est pas nécessaire pour le guichetier dont le besoin est réduit à une simple fonction de signalement.

4.2.5. Obligations de chaque responsable (participants, gestionnaires de la liste,...) (articles 4, 9, 10 et 12 de la LVP)

Dans divers articles (4, 9, 10, 12), la LVP définit essentiellement les obligations du responsable du traitement . Elle ne prend pas en compte la complexité des intervenants (participants, gestionnaires de la liste,...), qui ne revêtent pas nécessairement la qualité de responsable de traitement , dans la mise en oeuvre d'une liste noire. Dans l'intérêt des personnes enregistrées, il faut veiller à ce qu'aucun responsable d'une liste noire (participant, organisateur,...) ne puisse s'abriter derrière, soit des sous-traitants, soit des tiers, pour ne pas remplir ses obligations.

Les obligations respectives du responsable du traitement et de ceux qui alimentent et/ou consultent la base de données doivent donc être clairement définies par rapport au fonctionnement de la liste noire, de crainte que certaines exigences de la LVP elle-même ne soient pas satisfaites.

Par exemple, s'agissant de l'exactitude des données enregistrées qui serait contestée, la Commission estime que le responsable de base de données centralisée ne peut renvoyer la personne concernée auprès de celui qui a alimenté la liste des données contestées. A défaut de justification, dans un délai raisonnable, par celui qui a alimenté la liste, les données suspectes devraient être radiées.

Proposition normative additionnelle:

Un encadrement normatif doit, dans le chef de tous les acteurs impliqués directement ou indirectement dans les listes noires, requérir complémentairement des obligations plus spécifiques, telles que:

a) la détermination des responsabilités respectives faite en conformité avec les critères de la LVP

Etant donné que les listes noires impliquent des co-responsabilités (plusieurs acteurs fixent ensemble le but et les moyens de la communication et de l'enregistrement dans la liste noire), il s'impose que les acteurs privés prennent les dispositions qui permettent de déterminer celui qui endossera la qualité de responsable de la liste noire, le cas échéant, celles de sous-traitant et de tiers au sens de l'article 1er de la LVP et de définir la répartition des tâches entre les acteurs;

b) une mission précise d'information à l'égard des personnes physiques concernées;

c) la possibilité pour le citoyen de s'adresser à chaque participant pour exercer ses droits (accès, correction et/ou opposition).

Il serait indiqué qu'en cas de non-respect des obligations précitées, les données de la personne concernée soient immédiatement supprimées.

4.2.6. Principe de transparence (articles 9 et 17 de la LVP)

Dans la LVP, le législateur a intégré le «principe de transparence», tant sous la forme d'un devoir d'information (article 9 de la LVP) que par l'obligation de déclaration auprès de la Commission (article 17 de la LVP). Les risques liés aux listes noires peuvent justifier des exigences spéciales de transparence pour certaines listes noires dans le secteur privé.

a. Obligation de communiquer une information à la personne, entre autres, sur la motivation

A l'article 9, la LVP mentionne les obligations du responsable du traitement relatives aux informations à fournir à la personne concernée au moment où les données sont collectées (§ 1er) ou enregistrées (§ 2). Rien n'est prévu par la suite, lors de l'évolution des données.

De son côté, l'article 3, § 5, 4° de la LVP prévoit une exception au devoir d'information pour les traitements (en ce compris les listes noires) rendus nécessaires par la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux. Concrètement, ceci signifie que vu leur devoir de «compliance», les responsables des listes noires dans les établissements de crédit pourraient se référer à cette exception au devoir d'information immédiate prévu par l'article 9, sans préjudice de l'application de l'article 13 de la LVP. La Commission estime nécessaire de réglementer tous les aspects relatifs à la protection de la vie pri-

vée dans le cadre de l'application de la loi précitée de 1993 (voir ci-après).

Proposition normative additionnelle:

Une norme additionnelle pour les listes noires dans le secteur privé doit comprendre des obligations d'information plus spécifiques, telles que:

une information («ad hoc»), renouvelée et motivée donnée par le participant lorsque le fichage devient imminent mais qu'il peut encore être évité, et donc pas uniquement «a priori», sous forme de mention dans les conditions générales d'un fournisseur de services, par exemple. Lors d'un refus de service lié à un fichage par tout prestataire de service, la personne concernée doit également être clairement informée du motif du refus;

afin de permettre un contrôle judiciaire efficace de l'enregistrement sur la liste noire, il ne faut pas laisser à l'imagination des participants à la liste noire le soin de définir unilatéralement les divers critères d'enregistrement possibles, de les interpréter et/ou de les compléter. En vertu l'article 4, § 1, 2° de la LVP, les critères mentionnés dans la motivation «ad hoc» doivent être basés sur des critères qui sont décrits explicitement et limitativement dans la réglementation comme des raisons légitimes de l'enregistrement sur la liste noire (voir ci-dessus point 4.2.1.et 4.2.2.);

une information devrait être donnée par le responsable du traitement de la liste noire, pour chaque fichage (contrat, faits, etc.), et non pas seulement lors du premier enregistrement dans le fichier, comme c'est actuellement le cas pour la Centrale des Crédits;

en cas de modification importante des données , une information additionnelle devrait également être fournie d'office à la personne concernée. Elle pourrait ainsi mieux contrôler son image informationnelle.

Pourquoi disposer d'un droit de correction, si certaines données traitées sont ignorées dans les faits ?

pour les établissements de crédit chargés du devoir de «compliance» par la loi du 11 janvier 1993 précitée, l'autorité normative devrait prévoir l'obligation de mettre en œuvre un code spécifique en matière de protection de la vie privée pour toute liste noire nécessaire à la fonction de «compliance», et ce, en sus du processus en vigueur pour les autres listes noires utilisées dans ces établissements (par exemple, en application de la législation relative à la Centrale des Crédits aux Particuliers). Cette politique spécifique doit tenir compte de l'interposition de la Commission en vertu de l'article 13 de la LVP et des obligations que la LVP met à charge des établissements de crédit et qui ne tombent pas sous les exceptions limitées de l'article 3, § 5, 4° de la LVP.

b. Obligation de déclaration

L'article 17 impose au responsable d'un traitement automatisé d'en faire la déclaration auprès de la Commission, avant la mise en oeuvre du traitement.

Proposition normative additionnelle:

La Commission souhaiterait que des éléments supplémentaires soient mentionnés dans la déclaration lorsque le traitement envisagé est une liste noire:

– l'origine des données;

– le nom du ou des sous-traitants;

– les critères d'enregistrement (4.2.2.b);

– les noms des destinataires des données, lorsque ceci est possible plutôt que simplement les catégories de destinataires; à défaut, une liste de ceux-ci sera tenue à la disposition de la Commission.

Si l'une de ces exigences n'était pas respectée, les données de la personne enregis-

trée devraient être immédiatement effacées.

4.2.7. Les droits d'accès et de correction (articles 10 et 12 de la LVP)

L'article 10 de la LVP et l'article 32 de l'arrêté royal du 13 février 2001 portant exécution de la LVP règlent les modalités de l'exercice du droit d'accès à ses données par la personne concernée (aucune exigence de pli recommandé) ainsi que le délai de réponse (45 jours). En pratique, une réponse écrite est fournie.

Pour certains traitements, l'article 17bis permet au Roi, après avis de la Commission, d'obliger le responsable à désigner un préposé à la protection des données, chargé d'assurer, d'une manière indépendante, l'application de la loi et de ses mesures d'exécution et, notamment, de répondre aux demandes d'accès des personnes concernées.

L'article 12 de la LVP règle le droit de correction. Indépendamment de la possibilité de corriger des erreurs matérielles (par exemple, homonymie), ce droit implique la possibilité pour la personne concernée d'ajouter ses contestations et remarques pertinentes, aux informations enregistrées dans la liste noire.

Outre ces droits d'accès et de correction du citoyen, la LVP impose également des obligations en matière de contrôle d'accès et de correction des données (voir ci-après le point 4.2.11. «Sécurité et contrôle»).

L'article 3, § 5, 4° de la LVP prévoit une exception aux articles 10 et 12 pour les listes noires nécessitées par la loi du 11 janvier 1993, en sorte que les responsables peuvent se référer au devoir de «compliance».

Proposition normative additionnelle:

Une norme additionnelle pour les listes noires dans le secteur privé pourrait comprendre des obligations complémentaires, telles que:

a. Désignation d'une personne chargée de la sécurité et de la protection des données

La désignation d'une telle personne, chargée d'assurer le respect des règles applicables en la matière et susceptible de prendre en charge en première ligne le traitement des plaintes éventuelles, des demandes d'accès et/ou de correction, devrait être prévue dans un encadrement normatif (voir 4.2.4. a). Son rôle serait non seulement réactif mais également proactif.

b. Manière dont le droit d'accès / de correction doit être exercé

Il est de pratique courante d'imposer à la personne enregistrée, lors de l'exercice de son droit d'accès ou de correction à l'égard d'une liste noire, des exigences formelles qui dépassent ce que la LVP permet actuellement. Ainsi, il est fréquent d'exiger que la personne concernée exerce son droit d'accès par un courrier recommandé , alors que l'article 10 de la LVP impose uniquement une demande datée et signée.

Certains participants exigent même le paiement de frais administratifs pour accéder à une demande de communication des informations, ce qui est contraire à la LVP. Par conséquent, il conviendrait de préciser la manière selon laquelle la personne concernée peut exercer son droit d'accès.

c. Auprès de qui le droit d'accès / de correction peut être exercé

La complexité du système et de ses acteurs (participants, gestionnaires de la liste,...) rend la situation très compliquée pour la personne désireuse d'exercer ses droits. Si une liste noire est tenue à jour au niveau sectoriel, doit-elle s'adresser au siège de son prestataire de services, au guichet local du prestataire de services, ou au

gestionnaire externe éventuel de la liste noire ?

Au point 4.2.4. la Commission a défendu l'idée que la personne concernée doit avoir la possibilité de saisir chaque participant responsable de la communication et/ou du traitement ultérieur de ses données à caractère personnel de son droit d'accès et/ou de correction.

d. Abréviation des délais de réponse

La Commission estime que, vu les conséquences inhérentes aux listes noires, les délais de réponse à l'exercice des droits de l'article 10 de la LVP pourraient être notablement raccourcis. Dans la majorité des cas, un délai d'une quinzaine de jours est largement suffisant. Il pourrait en être de même pour le délai de correction sensu lato (article 12 LVP).

e. Contenu minimal de la réponse du responsable de la liste noire

L'article 10 de la LVP contient une liste des données qui doivent être communiquées par le responsable du traitement à la personne concernée. Ces informations essentielles ne sont pas toujours suffisantes pour expliquer aux personnes concernées la raison de leur enregistrement dans la liste noire et/ou leur permettre de le contester.

Les informations communiquées doivent être compréhensibles et, si nécessaire, expliquées. Un simple «print» d'une page de codes ne constitue pas une réponse satisfaisante.

En outre, la réponse au droit d'accès devrait, sauf dérogation éventuelle, systématiquement indiquer l'origine des données (traçabilité) (voir 4.2.8.).

4.2.8. Origine des données (articles 10 et 17, § 4 de la LVP)

L'article 10 de la LVP mentionne le droit, pour la personne qui exerce son droit d'accès, d'obtenir du responsable du traitement, outre la communication des données traitées sous une forme intelligible, celle de toute information disponible sur l'origine des données.

La Commission estime que l'enregistrement des données dans un fichier du type liste noire ne pourrait être autorisé sans que leur origine ne soit précisée (exigence de transparence) et donc, que celle-ci doit rester disponible pour les autorités de contrôle (par exemple, la Commission). La Commission considère qu'en matière de traitement de type «liste noire», une donnée d'origine incertaine est suspecte par nature et qu'en raison des conséquences susceptibles d'y être attachées, ne peut être maintenue.

Bien que la Commission considère que l'origine des données à caractère personnel doit être tenue à la disposition des autorités compétentes, elle insiste sur le fait que, dans des situations concrètes, après une mise en balance des intérêts respectifs, il pourrait être décidé de ne pas communiquer à l'intéressé des informations sur la source des données, lorsque l'existence d'un intérêt légitime à la protection de la source prévaut.

A cet égard, la Commission se réfère à la pratique analogue en matière de vérification des traitements gérés par les services de police en vue d'un contrôle d'identité (articles 13 de la LVP et 46 de l'arrêté royal du 13 février 2001 portant exécution de la LVP. Sur base de ces articles, après avoir contacté le responsable du traitement, la Commission fait le plus souvent part uniquement à la personne concernée que les vérifications nécessaires ont été effectuées. Dans certains cas, des informations complémentaires sont communiquées si la Commission les estime pertinentes et

opportunes (sans danger pour le protection de la finalité de la source).

Proposition normative additionnelle:

A défaut d'informations disponibles et satisfaisantes sur la source des données pour les autorités de contrôle, le cadre normatif devrait prévoir l'obligation de supprimer immédiatement la mention dans la liste noire.

4.2.9. Identification des personnes sur la base de données exactes et fiables et fraude d'identité (article 4, § 1er, 4° de la LVP)

L'article 4 de la LVP, mais aussi toute la philosophie de la loi, prônent l'exactitude des données fichées, en ce compris celles de l'identifiant. L'article 4, § 1er, 4° prescrit l'adoption, par le responsable du traitement, de toutes les mesures raisonnables (obligation de moyen) pour que les données inexactes soient effacées ou rectifiées.

Outre le fait de parer au risque d'homonymie, l'identification correcte et complète de la personne fichée concourt, également, à éviter qu'une personne totalement étrangère au fait qui a donné lieu à l'enregistrement n'en subisse les inconvénients.

Dans le cas des listes noires, et en raison des conséquences qui en résultent ou peuvent en résulter, la Commission estime que si des garanties sur la fiabilité des données ou leur caractère objectif ne peuvent être données, le fichage devrait être interdit.

Proposition normative additionnelle:

La Commission désire également évoquer le problème récurrent des personnes dont l'identité a été usurpée et qui sont victimes de fichage (fraude d'identité). A cet égard, une mention de la contestation et/ou de la qualité de victime d'une fraude d'identité devrait pouvoir être intégrée, conformément à l'article 15 de la LVP pour autant que la personne concernée ait donné son accord. Dans ce cas, seule l'information relative à la fraude d'identité pourrait être maintenue au-delà de la durée normale de conservation du fichage en vue d'éviter la multiplication des opérations frauduleuses.

4.2.10. Décisions automatisées (article 12bis de la LVP)

L'article 12bis de la LVP dispose qu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé, sauf lorsque la décision est prise dans le cadre contractuel ou est fondée sur une disposition prévue par la loi (...).

La Commission propose d'interdire d'appliquer cette exception relative au cadre contractuel pour les listes noires dans le secteur privé.

4.2.11. Sécurité et contrôle (article 16 de la LVP)

L'article 16 de la LVP impose un certain nombre d'obligations de sécurité et/ou de contrôle au responsable du traitement (et à son sous-traitant). Le § 4 de cet article dispose comme suit:

«Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous-traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel) contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces

mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

Sur avis de la Commission de la protection de la vie privée, le Roi peut édicter des normes appropriées en matière de sécurité informatique pour toutes ou certaines catégories de traitements.»

Cet aspect sécuritaire, à facettes multiples (technique, administratif, organisationnel), devrait être précisé, dans le cadre normatif, en fonction de la banque de données. La détermination des mesures de sécurité est essentielle pour la mise en oeuvre et le respect du principe de finalité.

a. Contrôle de l'accès aux données et utilisation de celles-ci

Le contrôle de l'accès par le responsable du traitement et par les participants au traitement implique des mesures organisationnelles et techniques à jour afin d'éviter un accès irrégulier. Ces mesures sont d'une importance capitale pour le contrôle du respect du principe de finalité.

Les mesures de contrôle d'accès devaient comprendre, notamment:

– un logging, c.-à-d. l'enregistrement de chaque consultation (sur quoi, par qui et quand?);

– un log-in personnalisé, c.-à-d. l'utilisation d'un mot de passe d'accès, spécifique à chaque collaborateur d'un participant;

– un contrôle d'accès pour les participants sur la base d'un inventaire des personnes habilitées à avoir accès aux données enregistrées et leur identification unique d'accès afin de contrôler leur consultation;

– la garantie d'une sécurité maximale, soit contre l'accès par des personnes non autorisées, en ce compris les membres du personnel des participants, soit contre l'accès à certaines données non autorisées;

– des contrôles effectifs par sondage et autres moyens doivent être exécutés.

b. Correction des données à caractère personnel

Une vérification constante de la qualité des données constitue l'une des obligations de base d'un responsable d'une liste noire. Il doit s'agir dans le domaine des listes noires d'une obligation de contrôle «proactif», au lieu d'un contrôle «réactif» activé uniquement à l'occasion d'une plainte.

Dans le domaine du fichage des crédits, la Commission constate que la plupart des situations dans lesquelles des données n'ont pas été correctement enregistrées dans la Centrale trouvent leur cause dans une défaillance de suivi ou une erreur de la part des prêteurs. Des exigences de rigueur accrue devraient être posées.

4.2.12. Transmission de données à caractère personnel vers des pays tiers (articles 21 et 22 de la LVP)

Il a déjà été précisé précédemment que l'application territoriale d'une liste noire peut être problématique au regard du principe de proportionnalité.

La Commission rappelle que les articles 21 et 22 de la LVP interdisent en principe la communication de données à caractère personnel sur des listes noires à des pays qui n'ont pas un niveau de protection adéquat.

Lorsqu'une entreprise conserve une liste noire, il peut y avoir une demande de transfert au sein d'une multinationale, d'un groupe d'entreprises, ou encore à des filiales, des sociétés soeurs ou une société mère dans des pays tiers. Dans ce cas, une attention particulière doit être accordée pour déterminer si le niveau de protection dans les pays tiers est adéquat et quelles sont les

législations qui y sont applicables A défaut de protection adéquate, il faut se conformer aux principes et exceptions de la LVP.

4.2.13. Contrôle par la commission

a. Avis de la Commission

Tout projet de norme relatif à une liste noire devrait être soumis à l'avis préalable de la Commission.

b. Autorisation préalable de listes noires spécifiques

Comme la Commission l'a déjà suggéré, une exigence d'autorisation préalable pourrait être imposée pour des listes noires spécifiques (voir 4.2.2.). En effet, la complexité de la mise en oeuvre d'une banque de données centralisée, et donc l'appréciation des compétences requises, justifie que les responsables de listes noires concernant des données dont le traitement porterait atteinte à un droit fondamental prévu par la Constitution ou à des services considérés comme essentiels par une autorités normative soient soumis à une autorisation préalable de la Commission.

c. Compétence de sanction

L'expérience de la Commission en matière de listes noires démontre une absence de sanctions. Or, on constate souvent que le responsable du traitement d'une liste noire a omis, de son propre chef, de respecter les obligations pour l'enregistrement et/ou la radiation de la liste noire. Généralement, cette constatation demeure sans conséquence financière pour lui. Cela donne, notamment, l'impression qu'une liste noire sans garanties efficaces pour la protection de la vie privée offre financièrement plus d'avantages qu'une liste noire qui exigerait plus de garanties et donc plus de moyens et que le «risque vie privée» juridique est financièrement insignifiant. C'est pourquoi, actuellement certains responsables estiment qu'il n'est pas vraiment nécessaire de consacrer des moyens importants à une politique efficace de protection de la vie privée.

Proposition normative additionnelle:

La Commission se réfère au point 4.2.4 où il est proposé de prévoir une recours avec effet suspensif auprès d'une autorité publique (par exemple, auprès du SPF Economie, Administration du Contrôle et de la Médiation) qui devrait disposer du droit d'appliquer des sanctions administratives en cas de fichage injustifié.

4.3. Formes d'encadrement

La Ministre de l'Emploi, chargée de la Protection de la Consommation, a demandé à la Commission quelle est finalement la méthode la plus appropriée pour réglementer les listes noires.

Comme elle l'a déjà mentionné dans son avis n° 11/2004 du 4 octobre 2004 , la Commission rappelle qu'une éventuelle réglementation des listes noires dans le secteur privé devrait répondre aux exigences formelles et de fond qui ont été formulées en la matière par la Convention européenne, la jurisprudence de la Cour européenne des Droits de l'Homme, la Constitution belge et enfin la LVP. Ainsi, non seulement la forme de la norme jouera un rôle mais également la qualité de l'encadrement normatif.

4.3.1. Article 8 de la Convention européenne des Droits de l'Homme

L'article 8 de la Convention européenne des Droits de l'Homme énonce que seule une loi peut prévoir des restrictions au droit de protection de la vie privée . L'expression «loi» à l'article 8 du CEDH n'exige toutefois pas qu'il s'agisse d'une loi au sens formel du terme. Il s'agit d'un concept de droit européen.

Selon la jurisprudence de la Cour européenne des Droits de l'Homme (voir notamment les affaires Sunday Time, Klass,

Malone et Kruslin), il doit être satisfait aux éléments de contenu suivants:

a) la limitation de la liberté doit se baser sur une nécessité sociale (donc pour établir la liste noire) et doit s'effectuer de manière proportionnelle.

Au moment d'évaluer l'exigence de nécessité sociale, l'autorité devra, notamment, veiller au caractère des services pour lesquels la liste noire serait instaurée et examiner dans quelle mesure la liste noire pourrait répondre à une nécessité sociale. Ainsi, il serait pertinent de vérifier si la liste noire compromet ou est susceptible de compromettre l'accès à des services essentiels et/ou des droits et libertés constitutionnels du citoyen.

b) la norme instaurée doit être suffisamment accessible et précise .

Premièrement, l'exigence «suffisamment accessible» implique qu'une information claire relative à la liste noire soit disponible.

Deuxièmement, les conditions et critères d'application de la liste noire doivent être suffisamment précis.

Autrement dit, les normes destinées à réglementer les listes noires devraient être libellées de manière à permettre aux personnes concernées d'adapter leur comportement à ces normes , compte tenu de leur situation précise (par exemple fraudeur, mauvais payeur, client à risque, auteur d'une protestation à l'encontre d'une facture, ...). C'est pourquoi on parle du critère de la prévisibilité . En d'autres termes, le principe de légalité institue une interdiction d'utilisation arbitraire de listes noires, pour n'importe quelle forme de risque client, par des entreprises privées.

Au moment d'évaluer l'exigence de prévisibilité, l'autorité normative devra veiller, notamment, à déterminer les informations à conserver sur les données enregistrées, les catégories de personnes visées, les circonstances de conservation des données, la durée de conservation et les catégories de destinataires et, à organiser un contrôle efficace du fonctionnement de ces listes noires, voire une sanction effective des responsables à défaut du respect de la réglementation applicable.

4.3.2. Article 22 de la Constitution

L'article 22 de notre Constitution stipule: «Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi».

La Commission a déjà rappelé dans son avis «Phénix» susmentionné que: «On sait que le Conseil d'Etat s'est déjà opposé à la création de traitements par simple arrêté royal et exige que les éléments essentiels des traitements du secteur public (finalité-type de données traitées) soient fixés par la loi elle-même».

De même, la jurisprudence constante de la Cour d'arbitrage dispose-t-elle, s'agissant de la portée des matières réservées par la Constitution à la loi comme tel est le cas de l'article 22 que, «bien que l'article 182 de la Constitution réserve la compétence normative au législateur fédéral, il n'exclut cependant pas que le législateur attribue un pouvoir limité d'exécution au Roi. Une délégation conférée au Roi n'est pas contraire au principe de légalité pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur» (C.A. n° 135/2004).

La Commission estime que, pour la mise en œuvre des listes noires dans le secteur privé, on doit, par principe, prendre en considération l'effet horizontal de l'article 22 de la Constitution, qui ne protège pas seulement le citoyen dans ses relations avec l'autorité, mais également dans ses relations avec son fournisseur privé de services. Le cadre normatif doit donc fixer avec pré-

cision les éléments essentiels des listes noires dans le secteur privé.

4.3.3. Conditions spéciales imposées par l'article 8 de la LVP

Compte tenu du caractère sensible des données à caractère personnel au sens de l'article 8, § 1er de la LVP («données judiciaires»), la LVP insère une interdiction légale de principe pour le traitement de telles données par un responsable du traitement dans le secteur privé.

En d'autres termes, selon la LVP, dans le secteur privé, le traitement de données à caractère personnel, sous la forme d'une liste noire, est en principe interdit si cette liste noire dépasse le contexte de la gestion interne des données (article 8, § 2 c) de la LVP). L'interdiction existe dès l'instant où des données à caractère personnel sont accessibles sous la forme d'une liste noire et d'une manière qui n'est plus nécessaire à la gestion du contentieux interne du responsable du traitement.

La LVP ajoute à cela, à l'article 8, § 4 que: «Le Roi fixe par arrêté délibéré en Conseil des ministres, après avis de la Commission de la protection de la vie privée, les conditions particulières auxquelles doit satisfaire le traitement des données à caractère personnel visées au § 1er».

4.3.4. Devoir d'information

Au point 4.1.3. d), il était déjà précisé que la LVP n'offre actuellement aucune base appropriée aux acteurs dans le secteur privé pour justifier une exception au devoir d'information. Toute dérogation sur ce point ne peut être réglée que par une loi. La Commission a fait remarquer qu'elle n'est certainement pas favorable à l'instauration de telles exceptions au devoir d'information dans le secteur privé.

PAR CES MOTIFS,

la Commission

confirme la nécessité d'un encadrement normatif des listes noires du secteur privé,

estime:

– en ce qui concerne la définition des listes noires, qu'il convient de se référer à la définition donnée par le Groupe 29, dans la mesure où celle-ci s'applique aux traitements de données du secteur privé permettant la communication de données à des tiers;

– qu'outre le respect des règles de la LVP, les principes mentionnés par la Commission doivent être pris en considération selon, éventuellement, le domaine d'application de la liste noire concernée;

– que les traitements du type «listes noires» doivent être régis par une loi qui en détermine les éléments essentiels de la manière la plus précise;

– que les traitements de ce type qui sont susceptibles de porter atteinte à un droit fondamental (article 23 de la Constitution) ou à un service considéré comme essentiel, doivent être subordonnés avant leur mise en oeuvre à une autorisation délivrée par la Commission;

– que les traitements de données visées aux articles 6, 7 et 8 de la LVP ne peuvent être mis en place qu'en conformité stricte avec les principes de la LVP, notamment, après l'adoption d'une loi spécifique qui les autorise;

– qu'en toutes hypothèses, les mesures d'exécution peuvent être confiées au Roi (arrêté royal délibéré en Conseil des ministres, précédé d'un avis de la Commission).

À propos de l'avis de la Commission de la protection de la vie privée du 15 juin 2005 sur l'encadrement des listes noires[1]

1. Les listes noires ne sont pas un phénomène nouveau, mais de nos jours, cette pratique tend à s'étendre. Assurances, banques, associations patronales, associations de propriétaires, grandes surfaces, salles de jeux, fournisseurs de téléphonie ou autres fournisseurs de communications électroniques, etc.[2], constituent autant d'acteurs utilisant ce type de fichier. Le législateur[3] semble vouloir s'emparer de cette délicate question afin d'encadrer les pratiques actuelles. Saisie par Madame la Ministre de l'Emploi, la Commission de la protection de la vie privée (CPVP) a émis, le 15 juin, un avis sur la nécessité et le contenu d'un encadrement législatif des listes noires.

Le présent article analyse ces pratiques au regard de la législation de protection des données à caractère personnel[4], écartant volontairement les questions de droit de la concurrence que posent les listes noires[5]. Dans un premier temps, nous tenterons de définir la notion de liste noire. Ensuite, seront passés en revue certains principes présents dans la législation de protection des données personnelles permettant d'encadrer, potentiellement du moins, ce phénomène. Pour finir, nous émettrons de brèves réflexions sur l'opportunité d'une intervention de l'État, le mode de régulation et son contenu. Cet avis nous offre également l'occasion d'éclaircir la notion de données judiciaires ou, pour être plus précis, de préciser le champ d'application de l'article 8 de la loi du 8 décembre 1992.

1. Qu'est-ce qu'une liste noire ?

1.1. Liste noire, une notion ambiguë et un débat délicat

1.1.1. Des frontières mal établies

2. La notion de liste noire est large et difficile à cerner avec précision. Une typologie utilisant comme critère distinctif les acteurs pouvant accéder aux données de la liste noire permet de dégager l'extension de cette notion. Premièrement, les fichiers internes sont à différencier des fichiers externes. Ensuite, au sein de cette dernière catégorie, trois nouvelles sous-catégories peuvent être dénombrées.

– Les *fichiers internes*, c'est-à-dire les fichiers dont les données ne seront utilisées et accessibles que par l'entreprise gérant cette base de données.

1. Commission pour la protection de la vie privée, 15 juin 2005, avis n° 09/2005 sur un encadrement des listes noires.
2. Cette liste n'est qu'illustrative. À titre d'exemples, d'autres listes noires existent : les avocats et architectes utilisent des listes de mauvais payeurs ; certains journaux publient des listes de pédophiles ou de coureurs dopés ; Test-Achats publie des listes de firmes douteuses ; les États européens et bientôt la Commission publieront des listes nories de compagnies d'aviation, etc.
3. Voy. la proposition de loi modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel en ce qui concerne les conditions générales de licéité des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1693/001 du 31 mars 2005. Également disponible sur le site de la Chambre des représentants : http://www.lachambre.be.
4. L. 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801. Pour toutes les références ultérieures à ce texte, nous utiliserons l'abréviation «LVP».
5. Sur ces questions, voy. J. LAFFINEUR, «Listes noires ou décisions blanches ?», *D.C.C.R.*, 2004, n° 65, p. 12.

– Les *fichiers externes*, c'est-à-dire les fichiers destinés à être alimentés et consultés par des entités plus nombreuses qu'une seule entreprise. Dans une majorité de cas, la base de données sera alimentée par chaque entreprise (responsable du traitement) et la gestion proprement dite de celle-ci sera attribuée à un organisme distinct. Suivant notre critère, les listes seront accessibles :
  i) soit uniquement à un groupe fermé d'entreprises (p. ex. à l'ensemble des entités du groupe Dexia, Axa ou autre ...) ;
  ii) soit à l'entièreté ou à la quasi totalité des membres d'un secteur[6] (comme c'est le cas du fichier Datassur pour les assureurs ou du fichier Préventel pour les opérateurs de mobilophonie, des listes propres au secteur de la grande distribution ou de celles tenues par la Banque nationale ou l'UPC accessibles aux institutions du secteur du crédit à la consommation, etc.) ;
  iii) soit, enfin, à plusieurs secteurs. Ces listes multisectorielles, voire universalistes, ont pour but de rassembler l'ensemble des informations sur une personne donnée tout secteur confondu ou de les rendre accessibles de manière large (p. ex., les listes noires de coureurs dopés publiées sur l'internet, ...)[7].

1.1.2. Tentative de définition

3. Dans un langage courant, une liste noire est un « fichier recensant des personnes indésirables »[8] ou, d'après la définition du *Petit Robert*, « une liste de gens à surveiller, à abattre ». Quant à la CPVP[9], elle se range derrière la définition donnée par le groupe dit de l'article 29[10] : « Les listes noires consistent à collecter et à diffuser certaines informations concernant un groupe donné de personnes, élaborées conformément à certains critères en fonction du type de liste noire dont il s'agit, *se traduisant en règle générale par des effets nocifs et préjudiciables pour les personnes qui y figurent*. Ces effets peuvent entraîner la discrimination d'un groupe de personnes en les *privant de toute possibilité d'accès à un service déterminé ou en nuisant à leur réputation* ».

La première partie de cette définition se contente de spécifier un traitement de données à caractère personnel. Par la suite, le groupe de l'article 29 avance son seul critère permettant de distinguer les listes noires des traite-

6. Pour une liste d'initiatives relatives à des listes noires dans le secteur des assurances, voy. J. DHONT, « Le traitement de données à caractère personnel dans le secteur d'assurances. La légalité des banques de données », *Rev. dr. U.L.B.*, 2000, pp. 320 et s.
7. Nous évoquons ici la question des listes noires largement publiées, y compris sur Internet, et dont le but est de « moraliser un secteur de la vie sociale ». On songe bien évidemment à la publication de la liste des sportifs surpris en état de dopage, liste dont un décret de la Communauté flamande décidait la création. Ce décret a été sévèrement critiqué par la Cour d'arbitrage (C.A., arrêt n° 16/2005) au nom de l'art. 22 de la Constitution consacrant le droit fondamental des citoyens à la vie privée.
8. Commission Nationale de l'Informatique et des Libertés (CNIL), *Rapport sur les listes noires*, Documentation française, novembre 2003, p. 5, disponible sur http://lesrapports.ladocumentationfrancaise.fr.
9. Avis cité, point 4.1.1.
10. Le groupe instauré par l'art. 29 de la directive 95/46/CE (Dir. 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281 du 23 novembre 1995, pp. 31-50), appelé dans la suite de l'article « groupe de l'article 29 », a émis un document de travail n° 65 sur les listes noires le 3 octobre 2002, 11118/02/FR/final, avis disponible sur le site de la Commission européenne à l'adresse : http://europa.eu.int/comm/justice_home/fsj/privacy/studies/index_en.htm.

ments de données «classiques», celui *d'effet nocif et préjudiciable pour les personnes y figurant*, et fait allusion à deux des finalités des listes noires: la restriction de l'accès à un service déterminé et la nuisance à la réputation d'une personne. Cette définition est à nos yeux lacunaire car elle aborde le problème via le contenu. De plus, par sa largesse, tout traitement de données à caractère personnel est susceptible de tomber dans cette définition[11]. Finalement la référence aux finalités n'est qu'implicite et secondaire, alors qu'elle devrait être le critère déterminant[12].

4. C'est d'ailleurs ce critère des finalités que la CNIL utilise dans son rapport pour distinguer les listes noires. Elle y avance les classifications suivantes (basées sur une finalité réelle ou déclarée): obtenir le règlement de la créance ou écarter les mauvais payeurs et écarter les clients à risques. Sur cette base, nous proposons de définir les listes noires comme des «fichiers constitués de données à caractère personnel dont la finalité est *soit* d'obtenir le règlement d'une créance ou de constater son non-paiement, *soit* de constater des anomalies, *soit* d'écarter des clients représentant un risque pour un ou plusieurs secteurs, l'entreprise ou le particulier, *soit* de nuire à la réputation d'une personne». La notion de risque devra s'interpréter de façon extensive et vise, par exemple, le risque de vol, fraude, faux, risque aggravé, etc.

Cette définition permettrait d'appréhender certaines listes pouvant prêter à interprétation si on utilise la définition restrictive du groupe de l'article 29. Ainsi, selon notre opinion, une liste de personnes ne désirant pas recevoir de polluriels pourrait se voir qualifiée ou non de liste noire suivant les finalités. Si le but de cette liste est d'exclure ces personnes d'un service en posant comme condition d'accès à ce service l'acceptation de messages publicitaires, on doit, selon nous, la qualifier de liste noire. Si, par contre, cette liste est conservée par un fournisseur d'accès ou de services pour, par exemple, appliquer des filtres spéciaux aux boîtes de réception qu'il héberge, la qualification de liste noire ne pourra pas être retenue.

De plus, en évitant de définir une liste noire par son objet, nous évitons d'écarter certaines listes positives qui, utilisées négativement, seront qualifiées de listes noires. Par exemple, une liste positive (ou blanche) de personnes payant effectivement les remboursements d'un crédit qu'elles ont contracté peut aussi avoir des effets préjudiciables. Il suffit pour l'entreprise responsable de la liste de vérifier si la personne, cliente chez elle, est présente sur la liste positive pour, *a contrario*, savoir qu'elle n'est pas un «bon payeur» si elle n'y figure pas. Un même effet pourrait donc être atteint tant par une liste blanche utilisée de façon négative que par une liste noire consultée positivement. En résumé, ce qui caractérise une liste noire est l'utilisation qui va être faite des données qu'elle contient (et non son contenu), et par conséquent la finalité du traitement.

5. Cette approche par les finalités nous amène à poser la question suivante: faut-il traiter de la même manière les «listes noires» dont la finalité est de prévenir la fraude et celles dont la finalité est de constater la non-exécution d'un simple devoir contractuel,

11. En effet, la première phrase de cette définition pourrait comprendre tout traitement de données à caractère personnel, car il est possible d'argumenter que par nature, tout traitement de données a un caractère privacide et emporte donc des effets négatifs pour la personne fichée.
12. Quant à la deuxième phrase de cette définition, elle cite deux des finalités des listes noires et exclut donc potentiellement toutes les autres listes noires présentant des finalités autres, bien que le terme «peuvent» fait référence à une liste ouverte.

c'est-à-dire le non-paiement d'une obligation? Ne devraient-elles pas se voir appliquer un régime particulier? Les deux finalités ne doivent-elles pas être distinguées? Le risque de voir apparaître des «casiers judiciaires privés» encourage la prise de garanties supplémentaires pour ce premier type de fichiers. Y invite en outre, mais nous reviendrons sur ce point (*infra*, n° 19 et s.), la disposition particulière de l'article 8 de notre loi qui prévoit un régime particulier pour les données dites «judiciaires».

1.2. Analyse des intérêts poursuivis par les listes noires et des dangers créés par elles

6. La question de la légitimité de la pratique des listes noires se résoud par une mise en balance d'intérêts divergents[13], car ces pratiques sont à la fois nécessaires pour le secteur industriel afin de se prémunir contre certains clients, apprécier le montant demandé en échange de certains services et, parallèlement, faute d'encadrement, elles peuvent rapidement se montrer «privaticides». Dans les paragraphes qui suivent, nous allons tenter de lister quelques arguments souvent invoqués «pour et contre» les listes noires.

1.2.1. Des arguments en faveur des listes noires

7. Premièrement, les responsables de traitement avancent souvent les arguments suivants à propos de leurs propres listes noires: soumises à la loi du marché, les entreprises doivent, pour être concurrentielles, proposer les prix les plus bas possibles. Pour fixer ce prix, un calcul du risque que représente le client est nécessaire. À cette fin, elles ont un intérêt légitime à se protéger contre les clients à risque, ceci représentant pour elles une nécessité économique[14]. De plus, la liberté d'entreprise et du commerce leur permet dans une certaine mesure de gérer librement leurs affaires. L'obligation légale d'information[15] qui s'impose aux compagnies d'assurance doit également être signalée. Celle-ci les oblige à contrôler les données transmises par le candidat à l'assurance afin de leur permettre «d'une part, d'apprécier correctement le risque et de faire une prime équitable pour tous et, d'autre part, de lutter contre la fraude à l'assurance»[16]. Ces finalités ont d'ailleurs été considérées comme légitimes par le juge des référés du tribunal de Bruxelles dans une affaire *Datassur*[17], nonobstant l'avis de la Commission de la protection de la vie privée[18].

Au-delà de l'entreprise, un secteur tout entier peut avoir un intérêt légitime à se protéger contre les débiteurs défaillants et les pratiques frauduleuses dont sont victimes leurs membres qui, si elles se répandaient, pourraient remettre en cause le bon fonctionnement de l'ensemble du secteur et compromettraient les intérêts de la clientèle du secteur, voire l'image de marque d'un secteur considéré comme insuffisamment

13. Voy., à ce propos, l'avis très nuancé du groupe de l'article 29 déjà cité.
14. «Le système d'assurance basé sur la solidarité organisée entre assurés, ainsi que la concurrence nécessitent que les assureurs puissent évaluer le risque économique qu'ils encourent» (J. DHONT, *op. cit.*, pp. 320 et s.).
15. L. 25 juin 1992 sur le contrat d'assurance terrestre, art. 5, *M.B.*, 20 août 1992, p. 18283.
16. Civ. Bruxelles (réf.), 19 décembre 2000, *Bull. ass.*, 2001, p. 266, note C.-A. van OLDENEEL, pp. 277-281; voy. égal. B. DUBUISSON, «Secrets, mensonges et confidences – Conclusions», *Rev. dr. U.L.B.*, 2000, p. 364.
17. Civ. Bruxelles (réf.), 19 décembre 2000, *op. cit.*; Civ. Nivelles (réf.), 28 mars 2003, inédit; Civ. Bruges (réf.), 31 octobre 2001, inédit; Civ. Bruxelles (réf.) (8° ch.), 11 juin 2004, inédit.
18. CPVP, avis d'initiative n° 21/2000 relatif au fichier RSR (fichier ayant pour but le signalement, entre compagnies d'assurance, des risques spéciaux en assurances incendie, accidents et risques divers) géré par le Groupement d'intérêt économique Datassur.

attentif à bien sélectionner sa clientèle. Citons, par exemple, les listes noires des établissements de jeux de hasard empêchant l'accès aux personnes suspectées de tricherie à ce type d'établissement ou celles du secteur mobilophonique faisant la chasse aux fraudeurs.

8. Finalement, du côté des personnes fichées, la pratique présente aussi certains avantages. Dans le secteur du crédit par exemple, elle permet de lutter contre le surendettement en offrant aux éventuels nouveaux prêteurs la possibilité de consulter l'état d'endettement du candidat. À titre d'illustration, nous pouvons citer la réglementation concernant la Centrale des Crédits aux Particuliers[19]. Cette réglementation met en place deux volets, l'un dit positif et l'autre dit négatif. Le volet négatif vise l'enregistrement de tous les contrats de crédit à la consommation et de tous les contrats de crédit hypothécaire qui connaissent des défauts de paiement. Le volet positif quant à lui vise l'enregistrement de tous les contrats à la consommation et de tous les contrats de crédit hypothécaire souscrits. Préalablement à la conclusion d'un nouveau contrat de crédit, les entités concernées consulteront ces bases de données afin d'obtenir une information complète sur l'existence éventuelle d'autres contrats de crédit et leur hypothétique défaut de paiement. Ce système fondé sur une double liste permet de lutter contre le surendettement en permettant au prêteur de juger du niveau de solvabilité, d'endettement de l'emprunteur.

1.2.2. Des arguments contre les listes noires[20]

9. Comme le relève la Commission, les listes noires comportent certains aspects négatifs: «(1) la masse de données enregistrées dans certaines banques empêche un contrôle réel et efficace de la qualité des données; (2) des violations de confidentialité et l'absence d'identification de leur(s) auteurs sont rendues possibles par une sécurité insuffisante et/ou un manque de formation des participants, particulièrement dans le chef des interlocuteurs directs ('au guichet') avec la personne fichée; (3) le fichage est détourné de sa finalité originelle. Une liste noire créée pour une finalité déterminée (par exemple, la lutte contre le surendettement) est également utilisée comme moyen de contrôle à l'égard des candidats à un emploi; (4) les erreurs humaines fréquentes dues à la complexité du système en place, l'inadéquation du système». On notera que les dispositions de la LVP, à condition qu'elles soient effectivement appliquées, permettent, comme nous le démontrerons plus bas, de résoudre ces différents problèmes.

10. Dans certains cas, les risques sont démultipliés par des facteurs aggravants tels que la mutualisation ou l'exclusion de services répondant à des besoins ou droits fondamentaux. Les risques sont alors de «*stigmatiser* une catégorie de la population qui peut rencontrer des difficultés parfois passagères, telle que la perte d'un emploi, une maladie grave, une évolution de la situation familiale, ...», *d'exclure* une partie de la population de services, de «besoins ou d'intérêts considérés comme essentiels à la vie en société»,

19. L. 10 août 2001 relative à la Centrale des Crédits aux Particuliers, *M.B.*, 25 septembre 2001, p. 32027 et A.R. 7 juillet 2002 réglementant la Centrale des Crédits aux Particuliers, *M.B.*, 19 juillet 2002, p. 32542.

20. Les associations de consommateurs se saisissent régulièrement du problème (voy. p. ex., «Des assurés fichés sans contrôle !», *Test-Achats*, 1er juillet 2000, disponible sur http://www.testachats.be/images/19/194821_attach.pdf).

« *d'affecter*, potentiellement, les intérêts d'une catégorie de citoyens en protégeant les intérêts d'une autre catégorie »[21].

1.2.3. De la nécessité d'une balance

11. De cet aperçu de la divergence d'intérêts à propos des listes noires, nous déduisons qu'une délicate mise en balance d'intérêts est nécessaire. Cet arbitrage devra être réalisé entre, d'une part, les aspects positifs de ces fichiers et, d'autre part, les dangers que ceux-ci peuvent représenter, notamment pour la vie privée. Actuellement, une telle mise en balance doit, selon le prescrit de l'article 5, *f)*, de la LVP, être réalisée *a priori* par le responsable du traitement et ce, sous le contrôle *a posteriori* du juge en cas de litige[22]. Étant donné l'ampleur que peuvent atteindre de tels traitements et les droits pouvant être affectés, ces garanties suffisent-elles ?

On ajoutera que cette mise en balance n'est pas simple[23] : la constitution d'une liste noire dans le secteur bancaire ou dans un secteur relatif à la fourniture d'énergie sera évaluée différemment s'il existe dans ce secteur pour la personne menacée d'exclusion le droit à réclamer un service minimal bancaire ou de fourniture d'énergie.

2. Rappel des principes applicables aux listes noires. La LVP est-elle suffisante ?

12. Dans l'état actuel du droit, la LVP permet déjà d'encadrer cette pratique. En effet, à condition de rentrer dans son champ d'application, principes de finalité, de légitimité, de loyauté, de proportionnalité et d'exactitude, droits d'information, d'accès et de rectification, obligation de déclaration, obligation de sécurité, ... sont autant d'outils permettant d'encadrer les listes noires. Certains points méritent cependant que l'on s'y attarde.

2.1. Conditions de légitimité du traitement et de son contenu imposées au responsable du traitement

2.1.1. Légitimité quant à l'existence du traitement

13. Le principe de légitimité du traitement permet d'encadrer les listes noires dans la mesure où d'une lecture combinée des articles 4 et 5 de la LVP, le fondement de légitimité d'un traitement doit rentrer nécessairement dans l'une des six hypothèses prévues par la loi. En ce qui concerne les listes noires internes, l'article 5, *b)*, permettra de les justifier dans un bon nombre de cas dans la mesure où le traitement sera jugé comme nécessaire à la bonne exécution du contrat ; ainsi la banque qui enregistre ses mauvais clients le justifiera par les nécessités du contrat et de son bon déroulement, de même si un bailleur enregistre le défaut de paiement des loyers qui lui sont dus.

Par contre, dans le cadre des listes externes, invoquer ce fondement de légitimité apparaît difficile à soutenir. D'autres bases de légitimation pour les listes noires externes sont alors à cher-

21. CPVP, 19 avril 2002, avis n° 52/2002 relatif à la constitution d'un fichier externe des locataires défaillants, disponible sur http://www.moniteur.be.
22. *Cf.* égal. le principe de proportionnalité sous-tendant l'art. 4, § 1, 3°, de la LVP : « § 1. Les données à caractère personnel doivent être : (...) 3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».
23. Pour illustrer la difficulté de cette mise en balance, comp. les concl. sur la légitimité du traitement de la CPVP dans son avis *Datassur* (*op. cit.*), et en sens opposé, les concl. du juge dans l'aff. *Datassur* (Civ. Bruxelles (réf.), 19 décembre 2000, *op. cit.*).

cher et, comme la CPVP l'identifie, les responsables de traitement invoquent régulièrement les points *a)* et *f)* de l'article 5 de la LVP. Nous allons donc nous attarder sur ces deux bases de légitimité.

a. Consentement légitimant le traitement[24]

Sur la notion de consentement comme fondement de légitimité

14. Le consentement permet-il de légitimer un traitement de données dans le cadre de listes noires? Notons d'abord que cela dépend des données traitées. Des régimes particuliers sont en effet prévus pour certaines catégories de données. C'est ainsi que si les données peuvent être qualifiées de «médicales ou sensibles», le consentement de la personne ne permettra de légitimer le traitement que s'il est écrit et peut être retiré à tout moment. À noter en outre que le Roi pourrait déterminer des cas où «l'interdiction de traiter des données sensibles relevant de l'article 6 de la LVP (les données relatives à la race, aux opinions philosophiques, religieuses, etc.) ne peut être levée par le consentement écrit de la personne concernée»[25] et que si les données sont qualifiées de données judiciaires, le consentement ne suffira pas à légitimer le traitement.

Sur les conditions du consentement

15. Une manifestation de volonté libre, spécifique et informée[26] est nécessaire pour légitimer le traitement. L'existence d'une *liberté* du consentement est souvent problématique car les sociétés gérant des listes noires utilisent souvent la formule du contrat d'adhésion. La Commission le souligne d'ailleurs à juste titre lorsqu'elle écrit que «l'exigence de la liberté du consentement (article 1 § 8 de la LVP) semble problématique si ce consentement constitue la condition pour obtenir un service essentiel à la personne concernée»[27]. De plus, ce consentement doit être *spécifique*, c'est-à-dire qu'il n'est accordé que pour une ou des finalités déterminées. Il ne pourra donc être étendu à des finalités autres que celles prévues lors de la conclusion du contrat. Quant au dernier critère qualitatif, celui du consentement *informé*, la Commission, dans son avis *Datassur*[28], écrit que «[...] la personne concernée n'a, en pratique, que rarement l'occasion de prendre connaissance des conditions générales avant de signer un contrat et que de ce fait elle n'est pas suffisamment informée». De plus, l'article 4 de la LVP stipule que «§ 1. Les données à caractère personnel doivent être: (...) 2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions

24. «Le traitement de données à caractère personnel ne peut être effectué que: *a)* lorsque la personne concernée a indubitablement donné son consentement» (art. 5, *a)*, LVP) et «par 'consentement de la personne concernée', on entend toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement» (art. 1, § 8, LVP).
25. Art. 6, § 2, dern. phrase, LVP. On peut facilement imaginer que ce soit le cas à propos de listes noires.
26. Comme l'exige la définition même du consentement tel que reprise par la LVP (voy. la définition, *supra*, note 24).
27. Par exemple, «le consentement à l'utilisation des données médicales lors de la conclusion d'une assurance solde restant dû comme condition pour contracter un prêt hypothécaire ou lors de la souscription d'une assurance obligatoire RC pour les véhicules motorisés, ...» (CPVP, 15 juin 2005, avis n° 09/2005 sur un encadrement des listes noires, disponible sur http://www.moniteur.be).
28. CPVP, 28 juin 2000, avis d'initiative n° 21/2000 relatif au fichier RSR (fichier ayant pour but le signalement, entre compagnies d'assurance, des risques spéciaux en assurances incendie, accidents et risques divers) géré par le Groupement d'intérêt économique «Datassur», disponible sur http://www.moniteur.be.

raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. (...)». Donc, poursuit la Commission, «même avec le consentement de l'intéressé, le fichage n'est licite que s'il rencontre les prévisions raisonnables de l'intéressé. Par conséquent, un consentement non suffisamment informé ne suffit pas à rendre le fichage licite». En conclusion, ne rencontrant que très rarement les conditions imposées par la loi, le consentement doit être écarté comme source de légitimité dans la majorité des listes noires.

b. Principe de proportionnalité : de la mise en balance de l'intérêt légitime du responsable du traitement et de l'intérêt du fiché

16. L'application du point *f)* de l'article 5 de la LVP comme fondement de la légitimité des listes noires externes est plus délicate à traiter : «Le traitement de données à caractère personnel ne peut être effectué, dit cet article, que : *f)* lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui peut prétendre à une protection au titre de la présente loi». Les conditions de l'article peuvent être détaillées comme suit. Premièrement, le responsable du traitement doit invoquer un intérêt légitime. La notion de responsable évoque à la fois, en ce qui concerne le traitement consistant en la transmission à l'origine de l'information figurant dans la liste noire, l'entité qui transmet la donnée et participe ainsi à l'alimentation de la base de données commune et, en ce qui concerne la liste elle-même, le gestionnaire de celle-ci. En l'espèce, sont souvent invoquées la gestion des risques contractuels et/ou la prévention de la fraude, autant de motifs pouvant être considérés comme légitimes tant pour la transmission des données que pour leur mutualisation[29]. Que ces mêmes arguments puissent être invoqués pour justifier la transmission aux tiers, à savoir l'entité ou les entités destinatrices de telles données, ne semble pas poser de questions. Deuxièmement, la finale de cet alinéa implique une mise en balance d'intérêts entre, d'une part, l'intérêt légitime du responsable du traitement et, d'autre part, l'intérêt ou les droits fondamentaux de la personne concernée.

17. Il est unanimement admis que si un droit ou une liberté fondamentale sont invoqués par la personne concernée, l'intérêt légitime du responsable du traitement devra être plus important que si la personne concernée invoque uniquement un intérêt légitime. «Plus est grande la protection envisagée au bénéfice d'une catégorie, et plus sont, potentiellement, affectés les intérêts de l'autre catégorie, de telle sorte que la balance à trouver entre les intérêts des uns et des autres revêt en l'espèce un caractère primordial (...)»[30], notait la Commission à propos d'une liste noire de locataires risquant d'être privés d'un droit fondamental consacré par la Constitution, à savoir le droit au logement consacré par l'article 23 de la Constitution. Le même raisonnement pourrait valoir pour le droit à l'éducation si des listes noires étaient établies par des institutions d'enseignement[31] et avaient pour effet de priver l'étudiant de son droit à l'enseignement.

29. Voy. *supra*, pt. 1.2.1.
30. CPVP, 19 avril 2002, avis n° 52/2002 relatif à la constitution d'un fichier externe des locataires défaillants, p. 2, disponible sur http://www.moniteur.be.
31. À l'inverse, à propos des listes noires mettant en cause de simples intérêts, celui d'obtenir un crédit ou une assurance, le raisonnement pourrait être différent.

Selon l'économie de la loi, c'est au responsable du traitement que revient la tâche de vérifier s'il dispose d'un fondement légitime lors de la création d'un traitement.

2.1.2. Légitimité quant au contenu du traitement

18. Une attention particulière doit être accordée au principe de proportionnalité de l'article 4, 3°[32], qui implique une mise en balance entre, d'une part, la finalité du traitement et, d'autre part, les types de données collectées. La doctrine admet que cet article est une émanation du principe de proportionnalité s'appliquant à l'entièreté de la matière et non seulement à l'article 5, *f)*. Une mise en balance d'intérêts devra avoir lieu quelle que soit la légitimité du traitement et les données collectées devront se limiter au strict nécessaire à l'accomplissement de la finalité déclarée.

2.1.3. Le cas particulier des données judiciaires

a. L'article 8, un article flou aux contours incertains

19. Une des questions centrales posées par l'existence des listes noires est la crainte d'une justice privée à l'égard de citoyens convaincus de non-respect d'obligations contractuelles ou, pire, de commission d'infractions et qui, sans autre forme de procès, se verraient exclus de toute possibilité d'obtenir un bien ou un service. De telles informations ne constituent-elles pas au sens de la LVP des informations tombant sous le coup de l'article 8 et dès lors soumises au régime sévère, c'est-à-dire l'interdiction de traitement sous réserve de quelques exceptions à interpréter restrictivement?

Bien que la Commission[33] ait conscience de l'importance d'une délimitation claire de la portée de l'article 8, on peut regretter qu'elle ne profite pas de cet avis pour définir avec clarté et précision ce qu'il faut entendre par «données judiciaires» visées par l'article 8 de la LVP. Cet article stipule que «§ 1. Le traitement de données à caractère personnel *relatives* [(1) *à* des litiges *soumis* aux cours et tribunaux ainsi qu'aux juridictions administratives], [(2) *à* des suspicions, des poursuites ou des condamnations ayant trait à des *infractions*], ou [(3) *à* des sanctions administratives ou de mesures de sûreté] est interdit» (chiffres, crochets et mises en forme ajoutés par les auteurs). Le texte vise donc trois cas distincts. D'emblée, il est utile de préciser que la première catégorie s'ordonne autour du critère de l'introduction d'une procédure devant les cours et tribunaux[34]. La délimitation du champ d'application de la deuxième catégorie («données relatives à des suspicions, des poursuites ou des condamnations ayant trait à des infractions») semble plus délicate et retiendra l'attention. Quant à la troisième, son extension ne fera pas l'objet de commentaires de notre part.

32. «§ 1. Les données à caractère personnel doivent être: 3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement».
33. «Le principe (voire la portée) de l'interdiction de traiter de telles données et les exceptions doivent être clairement définis» (CPVP, 15 juin 2005, avis n° 09/2005 sur un encadrement des listes noires, pt 4.1.3.c, disponible sur http://www.moniteur.be).
34. Cette précision apportée, il subsiste un grand nombre d'interrogations comme le relève J. DHONT: «À partir de quels moments les données relatives aux litiges soumis aux cours et tribunaux sont estimées être d'ordre judiciaire? Dès la citation ou dès la comparution? Est-ce que les instances disciplinaires sont visées par la loi? S'agit-il obligatoirement de procédures contentieuses? Quid des procédures gracieuse? ...» (*op. cit.*).

b. Des suspicions (...) ayant trait à des infractions?

20. Quel type d'informations le législateur a-t-il voulu comprendre dans la deuxième catégorie visée par l'article 8?

Première clarification: faut-il que les suspicions, poursuites et condamnations aient toutes trait à des infractions (1) ou la précision «ayant trait à des infractions» se limite-t-elle à la notion de condamnation (2)? Cette précision est d'importance, car si le terme suspicion se rattache uniquement à la notion d'infractions, le champ de cet article se trouve considérablement réduit. En effet, prenons l'exemple d'une liste noire consistant à lister les personnes suspectées de naviguer sur internet à titre personnel plus de x heures par jour durant les heures de bureau. Si la notion de suspicion est indépendante de celle d'infraction, le traitement de ce type de données pourrait éventuellement être interdit. Par contre, si les suspicions doivent avoir trait à des infractions, le régime de droit commun sera alors applicable. Plus simplement, si les données n'ont pas trait à des infractions (suspicion de faute contractuelle, de risque d'accidents, de non-remboursement d'une créance, etc.), le régime à appliquer est celui du droit commun de la LVP.

Nous penchons pour la première interprétation. Plusieurs arguments nous confortent dans cette interprétation. *Primo*, l'argument textuel: le terme «relatives» invite à analyser les différentes hypothèses énumérées auxquelles il fait référence. Or cette énumération est composée de trois éléments: relatives à des litiges; relatives (...) à des suspicions ...; relatives (...) à des sanctions administratives (...). Si le législateur avait voulu isoler le terme «ayant trait à des infractions» aux seules condamnations, il aurait dû faire précéder «des condamnations» par la préposition «à»[35].

Secundo, l'argument tiré des travaux préparatoires qui précise la portée de l'article 8. «La notion de 'suspicions, poursuites ou de condamnations relatives à des infractions' montre que l'article 8 ne s'applique pas uniquement aux condamnations pénales mais également aux données dont il ressort qu'une personne est soupçonnée ou poursuivie pour un délit»[36]. Suspicions, poursuites ou condamnations y sont vues comme un tout.

Tertio, l'argument tiré de textes internationaux: l'article 8 de la directive 46/95/CE que l'article 8 de notre loi transpose. Ce texte prévoit un régime spécifique uniquement pour les «données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté». La première catégorie vise donc l'ensemble des données relatives (ou ayant trait) à des infractions, en ce compris les suspicions, poursuites ou condamnations. N'est donc interdit que ce qui a trait à des infractions et non, par exemple, la liste relative à des personnes «suspectées de non-rentabilité» détenue par un établissement de jeux de hasard.

35. De plus, cet argument textuel français est aussi valable en néerlandais: «De verwerking van persoonsgegevens *inzake* geschillen voorgelegd aan hoven en rechtbanken alsook aan administratieve gerechten, *inzake* verdenkingen, vervolgingen of veroordelingen met betrekking tot misdrijven, of *inzake* administratieve sancties of veiligheidsmaatregelen, is verboden».

36. Voy. «Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données», *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1 du 20 mai 1998, p. 42. Également disponible sur www.lachambre.be, session 49.

c. Dans un cadre judiciaire?

21. Mais cette seconde catégorie vise-t-elle uniquement les suspicions, poursuites ou condamnations récoltées dans un cadre juridictionnel, en l'occurrence judiciaire? En d'autres termes, une liste de suspicions de fraudes bancaires tenue par un banquier tombe-t-elle dans le principe d'interdiction si elle n'est pas collectée dans le cadre de procédures judiciaires? À cette dernière question, nous répondons par l'affirmative. En effet, vu le postulat de rationalité du législateur, le critère distinctif de la catégorie de données judiciaires que nous analysons ne peut être identique à la première catégorie de données, celles des données relatives aux litiges soumis aux cours et tribunaux, sous peine de voir l'intérêt du deuxième alinéa fortement réduit. Si cela était le cas, cette deuxième énumération devrait être vue comme une précision de la première, ce qui est contraire à l'énumération découlant du terme «relative à».

d. Du champ de la notion d'infraction

22. Enfin, est-ce que l'idée des législateurs internationaux est de prévoir un régime spécifique pour ce qui a trait au champ pénal et uniquement à celui-ci? Une analyse des textes qui ont précédé la loi de 1992 revue en 1998, et dont notre loi s'inspire, permet de répondre à cette question. L'article 6 de la Convention n° 108 du Conseil de l'Europe[37] et les considérants de ce texte poussent à répondre par l'affirmative. La directive quant à elle énumère trois cas qui amènent à penser que le fait d'avoir énuméré distinctement les infractions et les condamnations pénales permettrait aux États membres d'appliquer ce régime d'exception à des infractions non pénales. Sans doute cette référence aux textes dont la loi belge s'est inspirée ne suffit point dans la mesure où la convention du Conseil de l'Europe et la directive ne prévoient qu'un minimum de garanties et que les États membres restent libres de prévoir un niveau de protection plus élevé[38].

Était-ce l'intention du législateur belge, lors de la modification de la loi en 1998, d'inclure dans les données judiciaires visées par l'article 8 les informations relatives à des infractions non pénales? Les travaux préparatoires de cette législation indiquent que «la notion de 'suspicions, poursuites ou de condamnations relatives à des infractions' montre que l'article 8 ne s'applique pas uniquement aux condamnations pénales mais également aux données dont il ressort qu'une personne est soupçonnée ou poursuivie pour un délit»[39]. Il faut souligner que le terme employé est celui de «délit». Les infractions non pénales et les contraventions ne seraient pas visées par cet article; seules les données relatives à des délits et des crimes sont donc à considérer comme données judiciaires au sens de l'article 8. De plus, le législateur a, semble-t-il, voulu étendre la notion de données judiciaires au-delà des condamnations pénales, mais à aucun

37. Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, signé à Strasbourg le 28 janvier 1981. Ce texte prévoit un régime particulier pour des «Catégories particulières de données». Il vise, entre autres, les «données à caractère personnel concernant des condamnations pénales» et uniquement celles-là. Le rapport explicatif en son pt 47 va d'ailleurs dans le même sens: «Par 'condamnations pénales', il y a lieu d'entendre: des condamnations fondées sur une loi pénale et dans le cadre d'une procédure pénale».
38. La Dir. 95/46/CE va même plus loin et prévoit expressément cette possibilité pour les législateurs nationaux.
39. Voy. «Projet de loi transposant la Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données», *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1 du 20 mai 1998, p. 42. Également disponible sur www.lachambre.be, session 49.

moment n'a envisagé de l'étendre à des infractions non pénales. La notion «d'infraction» renverrait donc au champ pénal exclusivement et non au non-respect d'obligations civiles.

23. Afin d'être complet sur la notion de données judiciaires et la légitimité de leur utilisation, l'arrêt du Conseil constitutionnel français[40] doit être mentionné. L'article 9 de la loi française prévoyait que «Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en place que par: (...) 3° Les personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi, dans les conditions prévues par la loi; (...)». C'est précisément l'hypothèse de la création de liste noire qui est visée par cet article. Le Conseil constitutionnel français déclara cet article «entaché d'incompétence négative» pour deux raisons: l'une parce qu'il contenait une délégation de pouvoirs inconstitutionnelle et l'autre parce que la définition donnée par l'article était ambiguë. Le caractère inconstitutionnel de la délégation de pouvoir que la loi réalise au profit de la CNIL, l'équivalent de notre CPVP, sera examiné plus loin (pt 3.). Par contre, le second motif de rejet par le Conseil constitutionnel mérite l'attention. Sur l'ambiguïté de la notion de «prévention et de lutte contre la fraude», le Conseil s'exprime comme suit: la disposition «est ambiguë quant aux infractions auxquelles s'applique le terme de fraude; elle laisse indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction; qu'elle ne dit rien sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux infractions».

L'arrêt français doit susciter une réflexion dans notre pays au moment où est envisagée une législation des listes noires. Le Conseil réclame une définition légale précise des données couvertes chez nous par l'article 8, en particulier cette catégorie vise-t-elle des informations sur la crainte de commissions d'infractions conservées par des entités privées et en dehors de tout contentieux judiciaire proprement dit? Par ailleurs, en cas de réponse positive à la première question, le Conseil exige que des garanties soient introduites par la loi sur la durée de conservation et les conditions de partage et cessions de telles données. Ces exigences nous semblent répondre aux exigences d'une loi «prévisible et proportionnée», exigences déduites du libellé même de l'article 8.2 de la CEDH par la jurisprudence de la Cour de Strasbourg. Ces mêmes exigences sont requises par la Cour d'arbitrage belge et dès lors, il faudra en tenir compte sous peine de voir la législation qui pourrait être proposée en Belgique encourir les mêmes critiques que celles adressées à la loi française.

e. Des causes de légitimité particulières aux données judiciaires

24. En résumé, on peut donc distinguer trois cas de données dont le traitement sera en principe interdit. Le premier vise toute donnée relative à des

40. Décision n° 2004-499 DC du 29 juillet 2004, Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi No 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (non conformité partielle), *Recueil*, p. 126; *J.O.F.R.*, 7 août 2004, p. 14087, disponible sur http://www.conseil-constitutionnel.fr/decision/2004/2004499/index.htm.

litiges *soumis* aux cours et tribunaux aussi bien civils que pénaux. Les données concernées sont uniquement celles qui peuvent être collectées à partir du moment où un litige est effectivement introduit. Le deuxième est plus large et vise à la fois les suspicions, poursuites et condamnations, *dans un cadre judiciaire ou non* mais uniquement *pour ce qui a trait à un délit ou crime*. Le troisième vise les sanctions administratives ou mesures de sûreté et n'appelle pas de commentaires particuliers.

Cependant, lorsqu'on est face à de telles données, le traitement reste possible si une des cinq hypothèses prévues par la loi est remplie. Comme annoncé plus haut, l'une d'entre elles va plus particulièrement retenir notre attention: la gestion de son propre contentieux[41]. Que recouvre réellement cette notion? Ce sont les données nécessaires pour intenter une procédure pénale, civile, administrative ou en vue d'une mesure de sûreté, ou celles qui constatent ces mêmes sanctions et condamnations. Nous pouvons citer en ce sens la Commission elle-même, qui, dans son avis *IFPI*[42], arrive à la conclusion que les conditions prévues par la LVP «permettent donc à une maison de disques, à l'IFPI ou à la SABAM de traiter des données relatives à une infraction précise qu'elles ont pu constater, *dans la mesure où elles se situent dans une phase au moins préparatoire à un litige*». Comme toute exception, celle-ci doit s'interpréter restrictivement. Par conséquent, la récolte de telles informations en dehors de toute préparation à une action en justice afin de constituer une liste noire ne trouve pas justification aux yeux de la LVP.

2.2. Des droits de la personne concernée et des obligations corrélatives du responsable du traitement

2.2.1. Droit d'information

25. Le régime légal prévu par la LVP repose sur le principe de transparence. Les personnes fichées doivent être informées, sauf rares exceptions, de ce fichage, du type d'informations collectées, du responsable du traitement, du partage du fichier, etc.[43]. Le droit à l'information constitue donc la pierre angulaire de la LVP et permet l'exercice effectif des autres droits subjectifs qui lui sont reconnus par la loi. Cette obligation d'information, sans d'ailleurs préciser les modalités de celle-ci, impose une information sur les possibilités d'être inscrit sur les listes noires au moment de la conclusion du contrat. Il est cependant dommage que cette information n'ait lieu que dans une phase préalable et soit souvent bien éloignée de l'éventuelle inscription sur la liste noire. De plus, actuellement, il est fort difficile pour un citoyen de gérer efficacement l'ensemble des données traitées, avec pour corollaire le risque d'être dans l'impossibilité d'exercer son droit d'accès ou de contestation.

2.2.2. Droit d'accès et de rectification

26. La LVP prévoit la possibilité pour le fiché d'accéder aux données contenues dans la base de données et de les rectifier si elles sont erronées. Ce droit devrait être renforcé pour éviter les conséquences catastrophiques liées à l'empêchement de souscrire à certains services considérés comme essentiels.

41. Le texte stipule que «§ 2. L'interdiction de traiter les données à caractère personnel visées au § 1er n'est pas applicable aux traitements effectués: (...) c) par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige».
42. Commission pour la protection de la vie privée, 12 novembre 2001, avis d'initiative n° 44/2001 concernant la comptabilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications, disponible sur http://www.moniteur.be.
43. Voy. art. 9, LVP.

2.2.3. Les systèmes de décisions automatisées

27. L'interdiction des traitements fondant une décision purement automatisée est prévue par l'article 12*bis* de la LVP[44]. Elle est liée à la condition que la décision ainsi prise affecte de manière significative la personne ou ait des effets juridiques envers elle. Dans la grande majorité des cas, les listes noires seront comprises dans cette interdiction. Certes, le législateur peut autoriser ce traitement dans certains cas. Il lui revient d'opérer la balance d'intérêts protection vie privée-intérêt légitime du traitement automatisé. Par contre, il nous semble qu'autoriser ce traitement sur la base d'un contrat est plus délicat, bien que l'obligation dans ce cas de prévoir des garanties (p. ex., le droit à un entretien) est prévue par la loi. Premièrement, les mêmes remarques que pour le consentement valent ici. Deuxièmement, comment justifier la liberté de la personne de contracter pour des services considérés comme essentiels ou découlant de droits fondamentaux?

Au-delà, même si la consultation d'une liste noire n'entraîne pas une prise de décision automatique, on conçoit que la personne qui doit prendre la décision d'accepter ou non un client repris sur la liste marque quelque hésitation. Et l'acceptation d'un tel client entraînera sans doute sa responsabilité s'il s'avère que le client malgré tout accepté s'avère par la suite un mauvais client. Bref, il serait sans doute utile que la personne concernée, du moins dans le cadre de listes externes[45], soit avertie, lorsqu'elle entre en contact avec une entreprise qui utilise ce type de liste, que celle-ci prendra, outre les informations collectées auprès du candidat client, des informations[46] auprès du responsable qui tient la liste noire.

2.2.4. Principe de sécurité : des obligations existantes ... mais peu respectées

28. Le principe de sécurité permet d'assurer à la fois l'intégrité des données et leur confidentialité par la mise en place de mesures organisationnelles (Qui peut décider de déposer une information? Qui peut la lire? Auprès de qui une contestation sur une donnée pourra-t-elle avoir lieu?, etc.) et techniques (mot de passe, encryptage de certaines communications, conservations des log-in et log-out des bases de données, etc.). De plus, une obligation de diligence est prévue concernant la mise à jour et l'exactitude des données. Sans entrer dans les détails, il faut rappeler que cette disposition liste une série d'obligations permettant de rencontrer nombre de craintes concernant la sécurité, craintes formulées à l'encontre des listes noires[47]; encore faut-il qu'elles soient respectées, ce qui n'est pas le cas dans tous les traitements que constituent les listes noires.

44. «Une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité. L'interdiction prévue à l'alinéa 1er ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance. Ce contrat ou cette disposition doivent contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue» (art. 12, LVP).
45. En cas d'utilisation de listes noires internes, on peut facilement concevoir que la personne déjà en relations d'affaires avec le responsable du traitement s'attende raisonnablement à ce que son contractant utilise des informations sur le passé contractuel du client et ses agissements.
46. À noter que l'art. 9 sur le devoir d'information de celui qui collecte des données auprès de la personne concernée n'oblige pas à délivrer ce type d' information.
47. Sur ces craintes, *supra*, n° 9.

3. Faut-il légiférer en la matière ?

3.1. Les fondements possibles d'une intervention législative

29. Sans nous prononcer à ce stade sur l'opportunité d'une intervention législative et son contenu, relevons les arguments sur lesquels pourrait s'appuyer une telle intervention.

Un premier argument est tiré de l'obligation positive[48] mise à charge des États par l'article 8 de la Convention européenne des droits de l'homme de garantir la protection de la vie privée et familiale[49]. Cette obligation se dégage d'une jurisprudence abondante de la Cour européenne de Strasbourg. L'article 22 de notre Constitution relaie cette obligation positive lorsqu'il stipule que « La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ». Comme le notent J. Vande Lanotte et Y. Haeck[50], c'est le devoir de l'État d'intervenir lorsqu'un droit fondamental est mis en cause par des pratiques privées ou administratives. Dans la mesure où les listes noires remettent en cause certains droits fondamentaux tels, par exemple, le droit au logement, le droit à l'emploi ou la liberté de circulation, l'intervention de l'État se justifie. On notera qu'un tel fondement ne justifie l'intervention réglementaire de l'État que dans une mesure très limitée et que la nécessité de démontrer l'atteinte à un droit fondamental peut ne pas être évidente. Ainsi, peut-on considérer que la liste noire qui pourrait priver un citoyen d'une possibilité de s'assurer met en cause un droit fondamental, rien n'est moins sûr, sauf à interpréter largement la notion de dignité humaine consacrée par l'article 23 de la Constitution.

30. Un autre fondement de l'intervention apparaît possible : l'article 20 de la directive stipule que « 1. Les États membres précisent les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et veillent à ce que ces traitements soient examinés avant leur mise en œuvre. 2. De tels examens préalables sont effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle. 3. Les États membres peuvent aussi procéder à un tel examen dans le cadre de l'élaboration soit d'une mesure du Parlement national, soit d'une mesure fondée sur une telle mesure législative, qui définisse la nature du traitement et fixe des garanties appropriées ». Il est à souligner que l'écriture de cette disposition visait précisément des traitements comme les listes noires, comme cela ressort du considérant 53 : « Considérant que, ce-

48. F. SUDRE (éd.), *Le droit au respect de la vie privée au sens de la CEDH*, Bruxelles, Nemesis/Bruylant, 2005, p. 27.

49. Nombre d'auteurs (voy. les nombreuses réf. cit. par P. DE HERT et S. GUTWIRTH, « Controletechnieken op de werkplaats : herbeschouwingen in het licht van persoonsgegevensbeschermingsrecht », *Orientatie*, 1993, n° 5, pp. 125 et s. et J. VANDE LANOTTE et Y. HAECK, « Het Europees verdrag tot bescherming van de rechten van de mens in Hoofdlijnen, Antwerpen, Maklu, 1997, pp. 186 et s. ; voy. égal. Cass., 27 février 2001, *Vigiles*, 2001, p. 153 et note P. DE HERT, à propos du placement d'une caméra vidéo dans un grand magasin, où la Cour fait référence à l'article 22 de la Constitution et semble donc accepter implicitement son effet horizontal) soutiennent également qu'en droit interne du moins, l'art. 8 a un effet horizontal, c'est-à-dire que le prescrit vaut aussi bien dans les relations entre particuliers et administrations qu'entre particuliers. L'avis annoté mentionne également l'effet horizontal de l'art. 22 comme fondement de l'intervention du législateur.

50. J. VAN de LANOTTE et Y. HAECK, *op. cit.*, pp. 186-196. Voy. aussi l'attendu de la Cour de Strasbourg : « (...) à cet engagement plutôt négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie familiale » (Cour eur. D.H., req. n° 6833/74, *Marckx c. Belgique*, arrêt du 3 juin 1979, § 31). Sur ces obligations positives et l'analyse des décisions strasbourgeoises, voy. H. VUYE, « Over vliegtuigen, luchthavens, lawaaihinder, milieuhinder en mensenrecten ... Welke rechtsbescherming bieden artikel 8 EVRM en artikel 22 Grondwet », *R.G.D.C.*, 2003, p. 490. *Cf.* égal. L. BYGRAEVE, « Data Protection Pursuant to the Right to Privacy in Human Rights Treaties », 2003, *Int. J.L. and Inf. Tech.*, 6, n° 3, p. 25.

pendant, certains traitements sont susceptibles de présenter des *risques particuliers au regard des droits et des libertés des personnes concernées*, du fait de leur nature, de leur portée ou de leurs finalités *telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat*, ou du fait de l'usage particulier d'une technologie nouvelle; qu'il appartient aux États membres, s'ils le souhaitent, de préciser dans leur législation de tels risques». On notera que l'approche hollandaise nous apparaît suivre l'article 20 de la directive[51]. Sans doute peut-on voir dans l'article 17*bis*[52] LVP la transposition de l'article 20 de la directive. À cette heure cependant, aucun arrêté royal n'a encore été pris sur cette base.

31. Un troisième argument pourrait plaider en faveur de l'intervention législative. Il s'inscrit à la suite de nos réflexions sur l'ambiguïté de la notion de données «juridictionnelles» visée à l'article 8 de notre loi de 1992. Sans doute avons nous cherché à démontrer que la notion de suspicion d'infractions ne devait pas s'étendre aux informations relatives au non-respect établi ou supposé de dispositions non pénales, mais il n'empêche qu'un régime stricte devrait encadrer, au-delà des seules suspicions d'infractions pénales, certaines données détenues par les responsables de traitement dans la mesure où on peut à la suite de la Commission considérer qu'elles présentent «un caractère plus dommageable et plus délicat encore, dans la mesure où elles n'ont pas été soumises à l'examen du juge ni à une quelconque procédure contradictoire»[53]. De plus, les limites fixées par la loi de 1992 au traitement des données judiciaires sont telles que leur traitement ne peut s'opérer pour un responsable de traitement privé que dans le cadre de la seule gestion de leur propre contentieux. De telles limites sont, nous semble-t-il, trop étroites dans la mesure où les entreprises doivent légitimement pouvoir seules, voire conjointement, prévenir la commission d'infractions dont elles seront les premières victimes. Que la loi nouvelle sur les listes noires soit l'occasion de modifier sur ce point la loi de 1992 à la fois en légitimant mais surtout en entourant le traitement de ces données juridictionnelles de sévères garanties peut également être avancé comme argument. On soulignera à nouveau que c'est à propos de ce point précis que le projet de loi français[54] a été attaqué devant le Conseil constitutionnel français et que, comme le relate l'avis de la Commission annoté, «les traitements destinés à lutter contre la fraude requerront[55] en France une disposition ad hoc, avec les garanties appropriées et spécifiques répondant aux exigences de la Constitution (française)».

51. Plus étonnant encore, le document de travail du Groupe européen de protection des données, dit de l'article 29, adopté le 3 octobre 2002, ne fait pas allusion à cet article, même si dans ses conclusions, il attire l'attention sur le fait qu'il existe des risques particuliers à propos de listes concernant un grand nombre de citoyens dans des secteurs d'importance majeure (les télécommunications et le secteur financier).
52. Le Roi détermine, après avis de la Commission de la protection de la vie privée, les catégories de traitements qui présentent des risques particuliers au regard des droits et libertés des personnes concernées et fixe, également sur proposition de la Commission de la protection de la vie privée, des conditions particulières pour garantir les droits et libertés des personnes concernées. [...]
53. CPVP, 15 juin 2005, avis n° 09/2005 sur un encadrement des listes noires, pt 4.1.3.c, disponible sur http://www.moniteur.be.
54. L'art. 9 de la loi française prévoyait que «Les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en place que par: (...) 3° Les personnes morales victimes d'infractions ou agissant pour le compte desdites victimes pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice subi, dans les conditions prévues par la loi (...)». C'est précisément l'hypothèse de la création de liste noire qui était visée par cet article.
55. Cette disposition n'a point encore été prise.

3.2. Quel contenu?

32. L'avis du Groupe dit de l'article 29 analyse de manière systématique l'application de la directive aux listes noires; l'avis de la Commission belge le fait également à propos de la loi de 1992. Il est patent que ces dispositions européennes et nationales bien appliquées pourraient résoudre nombre de problèmes rencontrés, comme nous le remarquions d'emblée. Ainsi, le principe de qualité des données oblige à limiter le traitement à des données adéquates, à ne pas les conserver au-delà d'une certaine durée. Le principe de transparence, à veiller à l'information des personnes concernées tant de l'existence du fichier «liste noire» que de sa communication lorsqu'elle est externe à l'entreprise. Le principe de sécurité veille à assurer, au-delà de l'intégrité des données, leur confidentialité et plaide pour des mesures organisationnelles. Un simple rappel de ces règles et l'exercice par la Commission de ses pouvoirs d'enquête et, le cas échéant, de dénonciation aux parquets peuvent-ils dès lors suffire?

33. La particularité des listes noires qui constituent un outil de décision vis-à-vis des personnes concernées, qu'elles soient internes ou externes, justifie sans doute des précautions supplémentaires que la Commission peut encadrer elle-même. L'exemple hollandais[56] d'un vade-mecum expliquant la signification précise des diverses dispositions de la loi appliquées aux listes noires est sans doute utile. Au-delà, la mise à disposition d'un questionnaire contenant une check-list spécifique[57] à remplir par les responsables de tels traitements et à notifier à l'autorité de protection, de même que la confection d'un modèle de clause d'information des personnes concernées sur l'existence des listes noires sont prévues par l'autorité néerlandaise de protection et sont sans doute utiles à introduire chez nous également. Faut-il aller plus loin?

56. Voy. le site http://www.cbpwet.nl/themadossiers/th_zwl_melden.stm.

57. La «*Checklist Zwarte Lijsten*» est présentée comme suit:
«De checklist 'Zwarte lijsten' biedt een eerste handreiking om een zwarte lijst zo zorgvuldig mogelijk in te richten. De checklist biedt toetsingsvragen die beantwoord dienen te worden om te kunnen voldoen aan de normen van de Wet bescherming persoonsgegevens.
Wat is het doel van de zwarte lijst?
Welke motieven maken de aanleg van de lijst noodzakelijk?
Welke criteria gelden voor plaatsing op een zwarte lijst, dus welke gedragingen komen daarvoor in aanmerking?
Hoe verifieert de verantwoordelijke of de gegevens juist en nauwkeurig zijn?
In hoeverre wordt de toegang voor de betrokkene voor bepaalde voorzieningen afgesneden en welke alternatieven resteren?
Hoe essentieel is de voorziening voor de betrokkene?
In hoeverre is het doel van de lijst te kwalificeren als een 'bedrijfs(tak)belang'?
In hoeverre weegt het belang van het bedrijf of de bedrijfstak op tegen de schade die een betrokkene oploopt als hij of zij op een zwarte lijst wordt geplaatst (proportionaliteit)?
Kan het doel niet langs andere weg bereikt worden (subsidiariteit)?
Onderzoekt de verantwoordelijke de reden van opname als de betrokkene, met wie hij een contractuele relatie wil aangaan, op een zwarte lijst voorkomt?
Op welke wijze en van wie worden de persoonsgegevens verkregen?
Welke waarborgen zijn er om te voorkomen dat niet meer gegevens worden verwerkt dan noodzakelijk?
Worden de persoonsgegevens verstrekt aan derde partijen?
Welke (organisatorische en technische) maatregelen heeft de verantwoordelijke getroffen om de persoonsgegevens op de zwarte lijst te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking?
Hoe en op welk moment wordt de betrokkene meegedeeld dat, en met welke reden, hij of zij op een zwarte lijst is geplaatst?
Wordt de reden van contractsweigering aan de betrokkene meegedeeld en op welke wijze?
Hoe kan de betrokkene zijn inzage- en correctierecht uitoefenen?
In welke gevallen wordt de betrokkene van de lijst verwijderd?
Hoe lang blijven de persoonsgegevens op de lijst staan?
Is er een protocol waarin het beleid met betrekking tot de zwarte lijst is vastgelegd?».

34. Sans doute, n'est-ce pas aux auteurs d'un article de doctrine de décider là où un débat démocratique se justifie, mais simplement de soumettre à ce débat quelques réflexions en ce domaine.

La loi actuelle présente face aux traitements que constituent les listes noires dites « externes » quelques lacunes pour permettre d'atteindre l'objectif souhaité de protection des données. La première concerne le devoir d'information lorsque communication d'une donnée est adressée au responsable de la liste noire externe. Sur ce point, la loi actuelle[58] n'oblige pas ce dernier à une information directe de la personne concernée. Il s'agirait d'obliger le responsable de la liste de prévenir la personne concernée de son enregistrement, comme c'est le cas pour la liste négative des débiteurs défaillants, liste tenue par la Banque nationale. À cela, pourrait s'ajouter une information d'office sur la consultation de listes noires externes avant d'accorder ou non un service ou la vente d'un bien (décision d'octroi de prêt ou de refus, p. ex.), en l'espèce les listes noires[59]. Autre point, l'interdiction de listes noires trans- ou multisectorielles même si sans doute le principe de finalité déterminée et spécifique peut suffire à ce propos. Il est difficile d'admettre qu'un même responsable croise des listes provenant de différents secteurs. La publication de listes noires par tous moyens, y compris les médias électroniques, même dans le cadre de la presse, pourrait être interdite. Enfin, pour des listes propres à un secteur comme Préventel ou Datassur, l'existence d'un service « indépendant » chargé de la réception des plaintes et de leur suivi apparaît nécessaire[60] tant les conséquences d'un fichage erroné, incomplet ou de données obsolètes sont importantes[61]. On pourrait, comme certains pays l'envisagent, sanctionner par des dommages et intérêts forfaitaires chaque consultation des listes noires non conformes aux prescrits de la loi, ce qui, d'une part, faciliterait le recours des personnes reprises sur de telles listes et, d'autre part, amènerait les responsables de telles listes à se mettre en conformité avec la loi.

35. Reste la question des traitements de données relatives à des infractions présumées, constatées ou jugées pour lesquels la loi hollandaise prévoit un régime spécial[62] et que la loi française envisageait de réglementer[63]. Le flou actuel dénoncé (*supra*, n° 19) et l'impraticabilité des solutions extensives

58. *Cf. supra*, nos réflexions à propos des termes «sauf si la personne en est déjà informée», utilisés à l'art. 9, § 2, qui pourraient permettre de considérer l'information donnée *in illo tempore* lors de la signature du contrat par le premier responsable avec la personne concernée, information sur une possibilité de transfert, comme suffisante dans le chef du responsable ultérieur. À noter que le règlement Datassur prévoit la notification par Datassur d'une information sur son enregistrement propre.

59. À noter que cette information pourrait se faire à deux moments du processus. Premièrement, au moment de la communication des données. Il s'agirait alors de prévenir la personne que les décisions la concernant peuvent être prises sur base d'une consultation de listes noires. Une autre solution serait d'inclure cette information dans la décision (éventuellement sous la forme d'une motivation).

60. À cet égard, on peut songer que cette fonction soit confiée au «préposé à la protection des données» dont l'existence est prévue à l'art. 17*bis* de la loi de 1992 sur le modèle allemand et encouragé par l'Union européenne. Cet article prône la création de «préposés à la protection des données» nommés par le responsable du traitement et «chargés d'assurer, d'une manière indépendante, l'application de la présente loi ainsi que de ces mesures d'exécution». Un arrêté royal devait être pris à cet égard. On regrettera sur ce point le silence du Roi.

61. On pourrait considérer que cette obligation se déduit de l'art. 16 de la loi de 1992 qui prescrit l'obligation de prendre des mesures de sécurité adéquates aux risques encourus par les personnes concernées du fait de leur traitement.

62. c'est la procédure dite du «voorafgaand onderzoek», c'est-à-dire de l'examen préalable par l'autorité néerlandaise de protection des données prévue sur base de l'art. 20 de la directive dans trois cas seulement: utilisation de numéros d'identification personnelle pour des communications au-delà des finalités de départ; collecte de données sans information préalable et communications de données pénales ou de données relatives à des comportements illicites ou répréhensibles. Ce dernier cas est celui ici visé des listes noires de données relatives à des infractions.

63. Il est à noter que dans ces deux pays, aucune réglementation des listes noires n'est envisagée au-delà de ces listes relatives à des infractions pénales.

données au champ d'application de l'article 8 de la loi de 1992, qui condamne des traitements nécessaires pour une entreprise ou pour un secteur qui désire loyalement lutter contre la criminalité, amènent le rejet de ces solutions dans la pratique. Bref, il faut clarifier et une réglementation est utile sur ce point. Une telle réglementation autoriserait certes explicitement le traitement de ces données par des entreprises privées ou des associations d'entreprises privées et ce, au-delà de la gestion de leur propre contentieux mais, dans le même temps, les soumettraient à de sévères conditions. Elle devrait notamment répondre à certaines qualités telles que celles dictées par l'article 8.2 de la CEDH et la jurisprudence qui en a suivi. On rappelle ainsi qu'« Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est *prévue par la loi* et qu'elle constitue une mesure qui, dans une société démocratique, est *nécessaire* à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

Cette réglementation doit être le fait de la loi. Il s'agit, première raison, de modifier la loi de 1992 et seule une loi peut le faire. Une autre raison est l'interprétation restrictive donnée à l'article 22 de la Constitution belge. Si en effet, l'article 8 de la CEDH n'exige pas une loi au sens formel, par contre, au niveau belge, le Conseil d'État et la Cour d'arbitrage ont précisé que le terme loi renvoyait bien à la loi au sens strict, d'acte du législatif. Le Conseil d'État, dans un avis déjà ancien[64] mais de manière constante depuis, détermine la répartition des compétences entre législatif et exécutif comme suit : « l'article 22 de la Constitution impose en particulier au législateur fédéral l'obligation de garantir la protection du droit au respect de la vie privée et familiale ; il est, à l'inverse, seul habilité à déterminer les cas et les conditions dans lesquels ce droit peut souffrir certaines restrictions[65] ». La Cour d'arbitrage, dans un arrêt du 21 décembre 2004[66], écrit que « Bien que, en utilisant le terme 'loi', l'article 8.2 de la Convention européenne précitée n'exige pas que l'ingérence qu'il permet soit prévue par une 'loi', au sens formel du terme, le même mot 'loi' utilisé à l'article 22 de la Constitution désigne une disposition législative. Cette exigence constitutionnelle s'impose au législateur belge, en vertu de l'article 53 de la Convention européenne, selon lequel les dispositions de la Convention ne peuvent être interprétées comme limitant ou portant atteinte aux droits de l'homme et aux libertés fondamentales reconnues notamment par le droit interne ». Si l'intervention de la loi est nécessaire pour modifier l'article 8 LVP, on peut considérer pour le reste que l'intervention de la loi est contenue dans la délégation au Roi de l'article 17*bis* LVP (voir *supra* n° 30).

36. Comment envisager le contenu de cette loi : faut-il déléguer à une autorisation de la Commission le soin de fixer les conditions de tels traitements ? Une telle délégation pose des problèmes au regard de nos principes consti-

64. Avis du conseil d'État : projet de loi organique des services de renseignement et de sécurité, *Doc. parl.*, Ch. Repr., sess. 1995-1996, n° 638/1, p. 31.

65. Voy égal. J. VELAERS, *De Grondwet en de Raad van State, afdeling wetgeving. Vijftig jaar adviezen aan wetgevende vergaderingen, in het licht van de rechtspraak van het Arbitragehof*, Antwerpen, Maklu, 1999, p. 154.

66. C.A., 21 décembre 2004, recours en annulation n° 202/2004 de la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête, introduit par l'a.s.b.l. Ligue des droits de l'homme et autres, disponible sur http://www.arbitrage.be.

tutionnels fixés par l'article 33[67] et fait de la Commission de la protection de la vie privée une autorité administrative soumise au contrôle du Conseil d'État du moins en ce qui concerne ce type d'intervention[68]. La pratique hollandaise directement inspirée de l'article 20 de la directive 95/46/CE[69] prévoit une procédure peut-être plus complexe mais plus respectueuse de nos principes constitutionnels et démocratiques. Il s'agit de contraindre les responsables de tels traitements à passer par une procédure d'examen préalable par l'autorité de contrôle, en l'occurrence la Commission de la protection de la vie privée. Celle-ci instruit le dossier et se charge en cas de doute de consulter les représentants des groupes intéressés. En cas de décision négative quant à un tel projet de traitement, le responsable qui a introduit le dossier peut recourir au ministre de la Justice pour faire annuler la décision de l'autorité. Cette procédure ouverte et de dialogue laisse en outre la dernière décision au politique.

37. Faut-il élargir le régime qui serait prévu pour ces listes particulières de lutte contre la fraude à d'autres listes[70], ainsi à des listes de simples mauvais payeurs qui pourraient, étant donné l'étendue du marché couvert par la liste et le domaine concerné, se voir privés d'un service ou d'un droit essentiel dans nos sociétés pour assurer la dignité humaine ou qui se verraient privés d'un droit fondamental? On sait que l'État dispose de différents moyens pour obtenir la garantie du respect de tels droits, ainsi le droit à un service universel ou à un minimum de moyens d'existence. Ainsi, les droits à des services bancaires, téléphoniques ou d'électricité dits minima ou universels, le droit à une couverture d'assurance vis-à-vis de certains risques ont été proclamés sur la base d'instruments parfois autres que réglementaires.

Une discussion sur les questions de l'interdiction ou non de listes noires dans certains secteurs ou sur la nécessité d'une réglementation spécifique à une liste noire sectorielle se pose donc dans un contexte de discussions politiques délicates: qui supporte les risques liés aux problèmes de débiteur défaillant, le fournisseur de biens et services, la collectivité des fournisseurs et/ou l'État? L'État doit-il s'octroyer le monopole de la mise sur pied d'une liste noire vu le bien ou service envisagé? La constatation de tels enjeux plaide pour une décision finale par les autorités constitutionnellement en charge des choix politiques, le législateur. On note que le législateur, en matière de crédit à la consommation, n'a pas hésité à intervenir pour encadrer les listes noires et créer sous son contrôle une liste gérée par la Banque nationale, liste dont les modalités de fonctionnement sont précisées par une loi. On peut imaginer qu'il intervienne à d'autres propos lorsqu'il s'agira de garantir l'accès à un service nécessaire à la dignité humaine ou à l'exercice d'un droit fondamental. Faut-il dans ce contexte dénier tout rôle à la Commission de la protection

67. À noter égal. en ce sens, les remarques du Conseil constitutionnel français dans la décision déjà mentionnée.
68. En effet, la Commission, dans la mesure de l'exercice de ses pouvoirs de décision, constitue une «autorité administrative» «dans la mesure où leur fonctionnement est déterminé et contrôlé par les pouvoirs publics et qu'elles peuvent prendre des décisions obligatoires à l'égard des tiers ...» (sur ces critères, voy. D. DE ROY, «Être ou ne pas être... autorité administrative. Vers de nouvelles questions existentielles pour les A.S.B.L. satellites des institutions communales?», *Rev. dr. commun.*, 2002, pp. 200 et s., et F. VANDENDRIESSSCHE, «De invulling van het begrip administratieve overheid na de arresten Gimvindus en BATC van het hof van Cassatie», *R.W.*, 2000-2001, pp. 497 et s.).
69. En particulier le § 2 de l'art. 20 cité *supra*.
70. On note que la CNIL, dans son dossier sur les listes noires, limite la réglementation envisagée à ces seules listes. Voy. Commission Nationale de l'Informatique et des Libertés (CNIL), «Rapport sur les listes noires», *op. cit.*, p. 5, disponible sur http://lesrapports.ladocumentationfrancaise.fr.

de la vie privée? N'est-ce pas son rôle[71], dans le cadre des notifications qu'elle reçoit quant à la création de listes noires tant dans le secteur public que privé, d'intervenir d'initiative[72] lorsqu'il appert que le traitement est «susceptible de présenter des risques particuliers au regard des droits et libertés des personnes concernées»? Le récent rattachement de la Commission au Parlement par la loi du 26 février 2003[73] favorise ce dialogue entre le législatif et l'autorité de protection des données et augure du bon suivi de telles initiatives si elles étaient prises.

71. D'ailleurs, le consid. 54 de la Dir. 95/46/CE sur la protection des données personnelles vise cette situation et suggère aux États membres cet examen préalable: «considérant que, au regard de tous les traitements mis en oeuvre dans la société, le nombre de ceux présentant de tels risques particuliers devrait être très restreint; que les États membres *doivent prévoir, pour ces traitements, un examen préalable à leur mise en oeuvre*, effectué par l'autorité de contrôle ou par le détaché à la protection des données en coopération avec celle-ci; que, à la suite de cet examen préalable, l'autorité de contrôle peut, selon le droit national dont elle relève, émettre un avis ou autoriser le traitement des données; (...)».
72. Comp. avec ce passage de l'avis de la Commission (avis n° 09/2005, pt 4.3.1, a). «Au moment d'évaluer l'exigence de nécessité sociale, l'autorité devra, notamment, veiller au caractère des services pour lesquels la liste noire serait instaurée et examiner dans quelle mesure la liste noire pourrait répondre à une nécessité sociale. Ainsi, il serait pertinent de vérifier si la liste noire compromet ou est susceptible de compromettre l'accès à des services essentiels et/ou des droits et libertés constitutionnels du citoyen».
73. L. 26 février 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée, *M.B.*, 26 juin 2003, p. 34416. L'art. 2 de cette loi modifie l'art. 23 de la loi du 8 décembre 1992 et stipule: «Il est institué auprès de la Chambre des représentants une Commission de la protection de la vie privée composée de (...)».